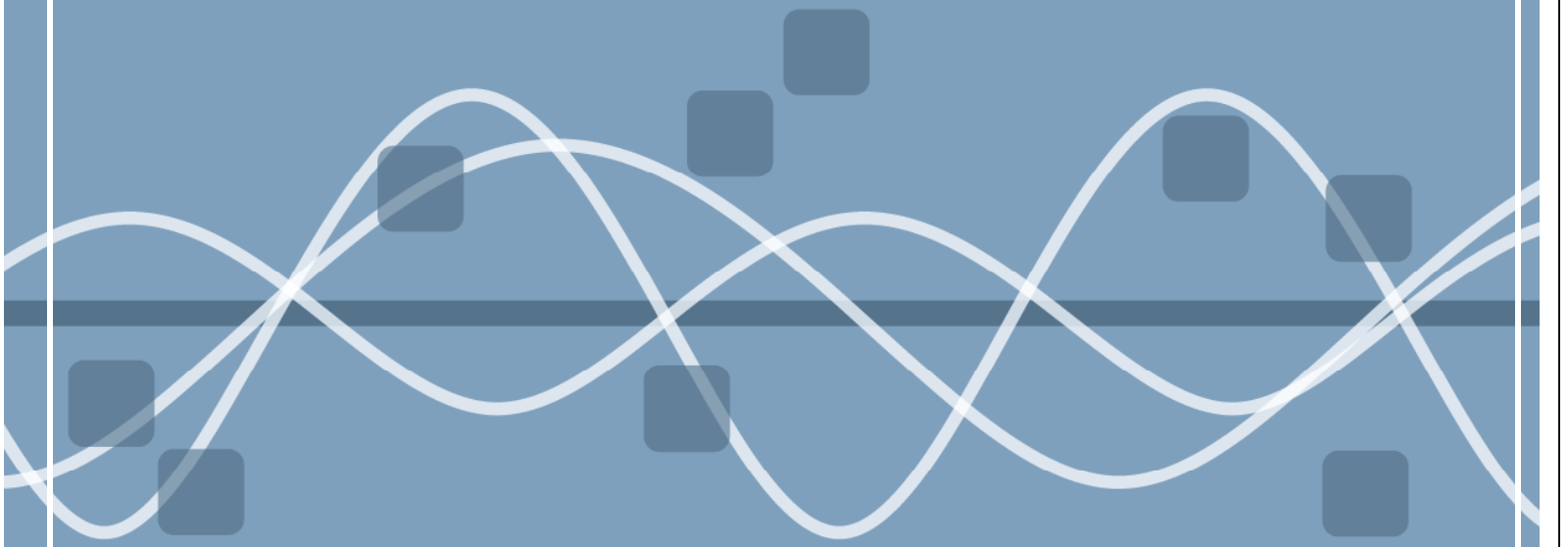
Standard du gouvernement du Québec
pour les ressources informationnelles
(SGQRI 34)

GUIDE POUR L'ÉLABORATION D'UNE POLITIQUE DE SÉCURITÉ DE L'INFORMATION NUMÉRIQUE ET DES ÉCHANGES ÉLECTRONIQUES

[*Pratique recommandée*]



Version [1.0]
Juillet 2003

Québec

COMPOSITION DU GROUPE DE TRAVAIL RESPONSABLE DE L'ÉLABORATION DE CE DOCUMENT

GROUPE DE SYNERGIE DU SSIGRI

Organisation	Participant
Direction du soutien au déploiement de l'inforoute Gouvernementale	Louise Thiboutot (Chargée de projet) Mohamed Darabid (Chef de projet) Max Chassé (Conseiller en sécurité de l'information numérique)

GROUPE DE TRAVAIL MINISTÉRIEL

Organisation	Participant
Ministère des régions	Jacques Roy
MJQ	André Tremblay
MRCI	Laszlo Czor
MRN	Claude Taillon
RAMQ	Maurice Gagnon
RRQ	Richard Bilodeau
	Pierre Bélisle
SAAQ	Mario Trudel

GROUPE D'INTÉRÊT (COSS)

Organisation	Participant
ANQ	Marc-André Leclerc
CF	Denis Aubé
CSST	Guy Rochette
Loto-Québec	Yves Leblanc
Hydro-Québec	Monelle Jeunehomme
MAM	Richard Gilbert
MJQ	Jeanne Proulx
MRCI	Marc Lafrance
MRCI (État civil)	Jacques St-Laurent
MRN	Marc Laurin
MRQ	Michel Leblanc
MSP	Bernard Dubois
MSSS	Philippe Moss
OPC	Yolande Côté
RAMQ	Michel Marchand
SAAQ	Claude Gélinas
SCT	Michel Després
SCT	Pierre Pouliot
SCT	Michel Rochette
SCT	Pierre Sasseville
SCT	Louise Thiboutot
SQ	Jean-Guy Pelletier Denis Rioux

TABLE DES MATIÈRES

1. Contexte d'élaboration du guide

Le Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles (SSIGRI) a pour mission de développer une vision gouvernementale de l'Administration électronique et de l'utilisation des technologies de l'information, de conseiller le Conseil du trésor et les instances décisionnelles dans l'exercice de sa gouverne de l'Administration électronique et des technologies de l'information, de fournir des services d'infrastructures communes aux ministères et organismes et de les appuyer et les accompagner dans la mise en œuvre de l'Administration électronique. Ce dernier volet se réalise entre autres dans l'élaboration et la mise en œuvre de pratiques gouvernementales de gestion de l'information et des technologies de l'information.

La volonté du gouvernement de s'engager dans la prestation électronique de services commande une réorganisation majeure de l'administration publique québécoise. L'un des enjeux majeurs d'un tel virage est la sécurité de l'information liée à ces services. Une telle entreprise appelle une formalisation des structures de responsabilité et des moyens de gestion de la sécurité de l'information. La préoccupation de la sécurité doit ainsi se retrouver dans les aspects de la gouvernance d'une organisation et, notamment, dans la définition des responsabilités, dans les processus de gestion et dans les mécanismes de contrôle et de suivi.

Le 4 février 2000 entrait en vigueur la *Directive sur la sécurité de l'information numérique et des échanges électroniques (CT 194055)*, adoptée le 23 novembre 1999 par le Conseil du trésor. Malgré qu'il appartienne d'abord aux ministères et organismes concernés de mettre en place les nouveaux éléments d'organisation et de gestion de la sécurité que commande la *Directive*, le Secrétariat du Conseil du trésor, par ses travaux sur la sécurité de l'information numérique et des échanges électroniques, a comme mandat de faciliter cette prise en charge.

Le présent guide portant sur l'élaboration d'une politique de sécurité de l'information numérique s'inscrit dans la portée de ces travaux. Il vise à créer un cadre de référence qui servira aux ministères et organismes pour l'élaboration de leur politique de sécurité interne. Le guide couvre aussi bien les objectifs de sécurité du DICAI (Disponibilité, Intégrité, Confidentialité, Authentification, Irrévocabilité) tels que véhiculés par la *Directive sur la sécurité de l'information numérique et des échanges électroniques* que les fonctions de Surveillance, d'Administration et d'Habilitation / Contrôle d'accès comprises dans l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN).

De plus, l'AGSIN a introduit au gouvernement du Québec le concept de domaine de confiance pour protéger l'information lors d'échanges électroniques. Le domaine de confiance repose sur une politique de sécurité et un cadre de gestion de la sécurité adéquats. Le présent guide vient donc supporter l'implantation de ce concept au gouvernement.

2. Organisation du guide

Le guide est constitué de 9 sections. Les sections 1, 2, et 3 traitent respectivement du contexte d'élaboration du guide, de son organisation ainsi que des acronymes et définitions.

La section 4 identifie les objectifs fondamentaux poursuivis par ce guide.

La section 5 définit les ministères et organismes visés par le guide. La section 6 précise les intervenants des ministères et organismes concernés par ce guide.

La section 7 traite du cadre réglementaire d'élaboration d'une politique en identifiant les lois générales, les lois spécifiques, les règlements et directives ainsi que les normes, les guides et standards pertinents à la sécurité des actifs informationnels. Elle traite également du processus d'élaboration des éléments constituants d'une politique de sécurité, de sa gestion et sa mise en œuvre. La section 8 est la conclusion du guide suivie des références à la section 9 et des annexes.

3. Acronymes et définitions

Voir lexique en annexe 1.

4. Objectifs fondamentaux du guide

Le présent guide vient soutenir les ministères et organismes (M/O) dans l'élaboration de leur politique de sécurité appuyant la réalisation de leur mission et la concrétisation de leurs objectifs stratégiques. Il identifie le contenu type recommandé pour une politique de sécurité et clarifie les étapes de sa production, de sa validation, de sa mise en œuvre, de sa diffusion et de sa gestion.

5. Champ d'application

Le présent document d'aide à l'élaboration d'une politique ministérielle de sécurité est recommandé aux ministères et aux organismes dont le budget de fonctionnement est voté, en totalité ou en partie, par l'Assemblée nationale ou dont le personnel est nommé et rémunéré suivant la Loi sur la fonction publique (chapitre F-3.1.1). Il est également recommandé à tout autre organisme public qui adhère à une infrastructure commune du gouvernement du Québec.

6. Clientèles cibles du guide

La clientèle ciblée par ce guide est constituée d'une variété d'intervenants qui ont pour tâche de contribuer, entre autres, à l'élaboration, à la validation ou à l'approbation du contenu de la politique de sécurité de leur organisation. Parmi ceux-ci, on retrouve :

- Les comités de sécurité;
- Les gestionnaires;
- Les détenteurs des actifs informationnels;
- Les responsables de la sécurité de l'information numérique (RSIN);
- Les spécialistes de la protection des renseignements personnels (PRP);
- Les vérificateurs internes;

- Les intervenants impliqués dans l'Architecture de sécurité de l'information numérique (ASIN);
- Les administrateurs de réseaux;
- Les spécialistes en technologies de l'information;
- Les conseillers juridiques;
- Les spécialistes de l'éthique;
- Les spécialistes en ressources humaines;
- Les spécialistes de la sécurité physique et matérielle.

7. Élaboration d'une politique de sécurité

Une politique de sécurité des actifs informationnels vise :

- La définition d'orientations stratégiques en matière de sécurité, appuyées par la haute direction, et la sensibilisation de l'organisation aux risques associés à l'usage des technologies de l'information et des échanges électroniques;

- L'utilisation adéquate des services de l'inforoute en soutien aux échanges électroniques;

- L'intégration de la gestion de la sécurité de l'information dans les processus d'affaires et dans le développement des systèmes d'informations ;

- La prescription et l'application de mesures de sécurité pour réduire les risques de préjudices et permettre aux ministères et organismes (M/O) d'atteindre les objectifs :

  - De disponibilité des actifs informationnels et de continuité des opérations;
  - D'intégrité des actifs informationnels;
  - De confidentialité de l'information sensible;
  - D'authentification des utilisateurs et, si besoin est, de l'irrévocabilité des actions et des documents électroniques qui en découlent.

7.1 Cadre légal et normatif d'élaboration de la politique

Le cadre d'élaboration de la politique de sécurité est constitué des lois, règlements, politiques, directives, normes, guides et standards dont les ministères et organismes doivent tenir compte lors de l'élaboration d'une politique de sécurité. Sans être exhaustifs, les principaux éléments à considérer sont :

- Les lois d'application générale tels le Code civil, le Code criminel, la Loi concernant le cadre juridique des technologies de l'information, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, etc.;

- Les lois d'application spécifique qui encadrent la mission d'un ministère ou d'un organisme. Exemple : Loi sur l'assurance hospitalisation; Loi sur les accidents de travail et les maladies professionnelles; Loi sur les régimes complémentaires de rentes; etc.;

- Les règlements, politiques et directives de nature interne ou externe. Exemple : Directive sur la sécurité de l'information numérique et des échanges électroniques du Secrétariat du Conseil du trésor (SCT); directive interne du ministère ou organisme sur l'utilisation d'Internet; etc.;

- Les normes, guides et standards : Normes ISO/IEC 17799; ISO/IEC TR-13335; AGSIN; etc.

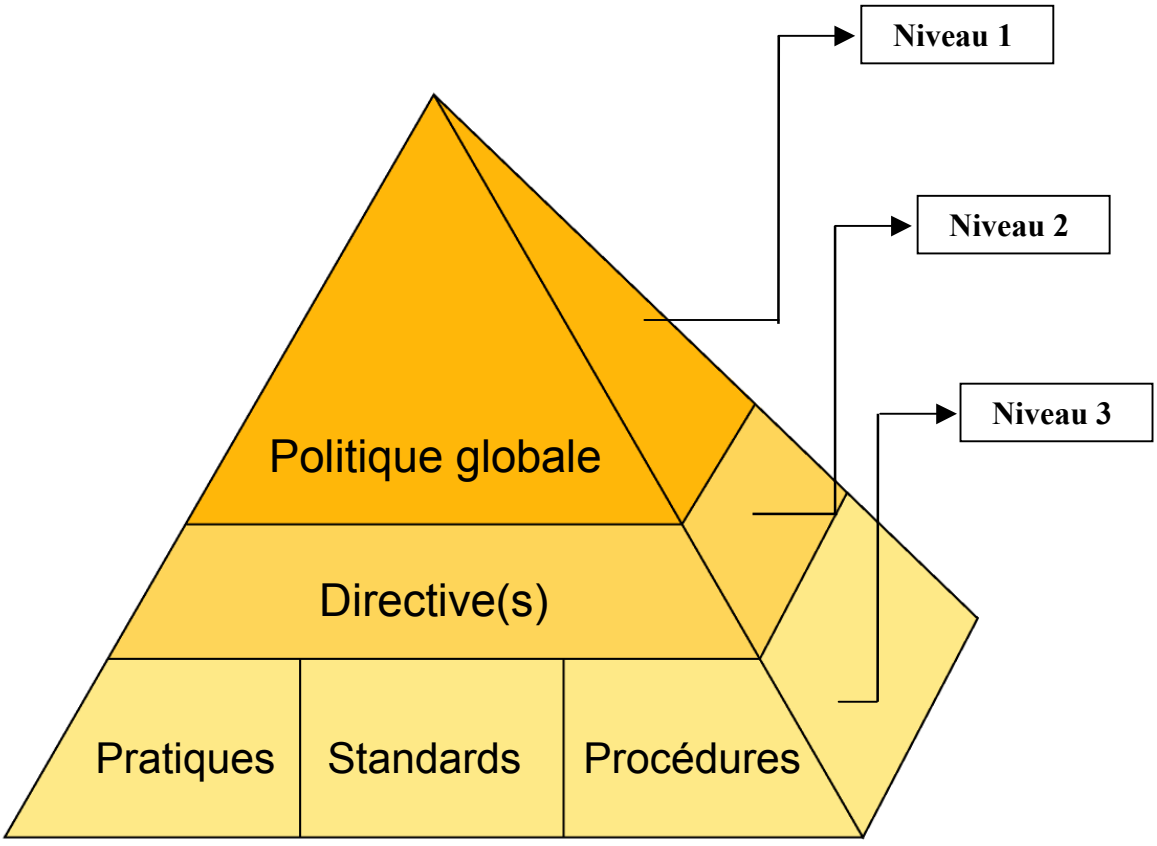
Une liste non exhaustive de ces lois, règlements, directives, normes, guides et standards est présentée en annexe 4.

7.2 Éléments constituants d'une politique de sécurité

La pratique recommandée pour l'élaboration d'une politique de sécurité repose sur les éléments suivants :

- Une politique globale;
- Une (ou des) directive (s) de sécurité;
- Des pratiques, standards et procédures.

Le schéma ci-après présente une hiérarchie des éléments constituants de la politique lesquels sont repris en détail dans les sous-sections suivantes :



7.2.1 Niveau 1 : Politique globale de sécurité

La politique globale de sécurité des actifs informationnels est, avant tout, la démonstration d'une prise de position ferme et claire d'un ministère et organisme quant à la sécurité à accorder aux actifs informationnels et aux échanges électroniques. Elle est constituée d'énoncés de principes généraux et de responsabilités aux fins :

- D'identifier les intervenants concernés et leurs rôles et responsabilités dans la gestion de la sécurité;
- De sensibiliser les utilisateurs aux risques associés à l'usage des technologies de l'information;
- De concevoir et d'implanter les mesures qui assurent efficacement la sécurité des actifs informationnels.

La politique globale est généralement élaborée sous la coordination du responsable de la sécurité de l'information numérique (RSIN) avec la participation active des intervenants clés[1]. La politique globale est sanctionnée par le sous-ministre ou le dirigeant de l'organisme.

Le contenu type d'une politique globale de sécurité est présenté à la section 7.5 du présent document.

7.2.2 Niveau 2 : Directives de sécurité

Les directives de sécurité viennent en appui à la politique globale de sécurité. Elles permettent de la développer et de la préciser. Elles déterminent, par des mesures concrètes, la façon de procéder en vue d'assurer la sécurité des actifs informationnels dans des domaines d'application particuliers. À titre d'exemple, on peut citer les directives suivantes :

- Directive sur l'utilisation des écrans de veille;
- Directive pour la sécurité des accès aux informations et aux infrastructures technologiques;
- Directive sur l'utilisation d'Internet;
- Directive sur la sécurité dans le développement des systèmes;
- Etc.,

En collaboration avec l'ensemble des directions impliquées dans la protection des actifs informationnels, une directive est généralement élaborée sous la coordination du

[1] Les responsabilités en matière d'élaboration, de mise en œuvre et de gestion de la politique globale sont définies par les ministères et organismes en fonction de leur propre organisation interne.

responsable de la sécurité de l'information numérique[2] La directive est ensuite sanctionnée par le sous-ministre ou son délégué.

Le contenu type d'une directive de sécurité des actifs informationnels est traité plus en détail dans la section 7.6 du présent document.

7.2.3 Niveau 3 : Pratiques, standards et procédures

a) Pratiques

Le sens donné par le présent document au terme « *pratique* » rejoint celui d'une « *bonne pratique* » dont le grand dictionnaire terminologique de la langue française en donne la définition suivante :

« Un 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 ».

Le cadre d'implantation des mesures de sécurité identifiées dans une directive de sécurité (niveau 2) est documenté dans une série de pratiques de sécurité. Les pratiques assurent que les contrôles de sécurité ainsi que les processus de support nécessaires sont implantés de façon consistante et correcte à travers l'organisation. Elles sont sanctionnées par le comité de sécurité du ministère ou organisme.

Une pratique de sécurité donnée peut être reliée hiérarchiquement à un énoncé d'une directive de sécurité en particulier mais cela ne représente qu'une minorité des cas. Étant donné que l'implantation de mesures de sécurité se fait généralement sur la base de tâches particulières à accomplir ou de zones d'activités opérationnelles spécifiques, les pratiques seront le plus souvent transversales; c'est-à-dire qu'elles seront reliées à plusieurs directives.

Exemple 1 : Une pratique concernant les logiciels antivirus pour postes de travail sera hiérarchiquement reliée à une directive de sécurité (niveau 2) portant sur les logiciels malicieux.

Exemple 2 : Une pratique sur la gestion des incidents de sécurité de l'information numérique peut être reliée à une directive sur l'utilisation du courrier électronique ou à celle portant sur la continuité des services.

[2] Les responsabilités en matière d'élaboration, de mise en œuvre et de gestion des directives sont définies par les ministères et organismes en fonction de leur propre organisation interne.

b) Standards

Pour une meilleure compréhension de la définition d'un standard, nous commencerons, en premier lieu par la définition d'une norme.

Selon l'ISO[3] une **norme** se définit par *« ....accords documentés 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.*

Les normes internationales contribuent ainsi à nous simplifier la vie et à accroître la fiabilité et l'efficacité des biens et services que nous utilisons. »

Selon l'Office de la langue française (OLF), **un standard, norme de facto ou norme de fait** se définit comme suit : *« Norme qui n'a pas été définie ni entérinée par un organisme officiel de normalisation comme l'ISO, le CCN[4], 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. »*

Toujours selon l'OLF, il est parfois conseillé de réserver le terme « norme » à celle qui est reconnue par un organisme officiel et « standard » à celle qui ne l'est pas, mais qui s'est imposée de soi.

Ainsi, la terminologie recommandée pour les travaux du gouvernement du Québec est la suivante :

- Le terme **« norme »** accompagné du qualificatif « internationale », « nationale » ou « européenne », signifie une norme reconnue par un organisme officiel.
- Le terme **« standard »** indique une « norme de facto ».

L'utilisation de normes et de standards permet de réduire la complexité des environnements et des opérations en uniformisant les éléments constituants d'un univers informationnel au sein d'une organisation et en facilitant les échanges avec l'extérieur. Les normes et standards fixent les bases architecturales des systèmes et fournissent un dénominateur commun pour l'évolution des actifs informationnels.

Les standards sont sanctionnés par le comité de sécurité du ministère ou organisme.

[3] ISO : Organisation internationale de normalisation
[4] CCN : Conseil canadien des normes

Exemple 1 : Utilisation généralisée et uniforme d'un système d'exploitation sur tous les serveurs d'une organisation.

Exemple 2 : Utilisation de la pratique standardisée sur les domaines de confiance au gouvernement du Québec.

c) Procédures

La définition par l'OLF du terme *« procédure »* est la suivante :

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

Les procédures décrivent en détail toutes les étapes d'un processus humain ou technologique d'implantation ou d'opération d'une mesure de sécurité. Les documents procéduraux sont normalement écrits et entretenus par les groupes responsables de leur exécution étant donné que le contenu de tels documents est largement dépendant de l'environnement, des outils utilisés, des personnes impliquées, etc.

Les procédures sont sanctionnées par la direction chargée de la gestion des ressources informationnelles du ministère ou organisme.

Exemple 1 : Procédure d'attribution ou de retrait d'un identifiant et des droits d'accès.

Exemple 2 : Procédure de destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation emmagasiné sur un support micro-informatique.

7.3 Étape préalable à l'élaboration d'une politique de sécurité

Certains éléments fondamentaux doivent être identifiés avant de commencer à élaborer une politique de sécurité respectueuse de la réalité du ministère ou de l'organisme concerné. Les sections suivantes traitent de ces éléments préalables.

7.3.1 Définition de la mission du ministère ou de l'organisme

La politique de sécurité vient appuyer la mission d'un ministère ou organisme notamment pour la réalisation des objectifs stratégiques qui en découlent. En contrepartie, la mission fournit aux intervenants en sécurité les indications pertinentes leur permettant d'identifier le type de clientèle visé et de classifier les actifs informationnels de l'organisation selon leur degré de sensibilité

Voici un exemple de mission :

L'Agence gouvernementale de la faune et des parcs [5] a pour mission :

- De fournir l'information générale sur la faune et les parcs et particulière sur la chasse;
- De permettre au citoyen de consulter son dossier personnalisé faisant état de sa situation personnelle de membre;
- De fournir en ligne le ou les permis désirés.

Note : Afin de pouvoir bénéficier de ces services, les citoyens doivent absolument s'inscrire comme membre du programme « chasse en ligne ». Il importe donc qu'un pareil processus soit strictement encadré sur le plan de la sécurité des actifs informationnels.

7.3.2 Définition du cycle de gestion de la sécurité

Tel que précisé dans le document intitulé *« Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise »*[6] et illustré par le schéma, joint en annexe 2, extrait de ce même document, les ministères et organismes doivent établir et maintenir leur propre cycle de gestion de la sécurité de l'information numérique arrimé au cycle de gestion gouvernemental.

7.3.3 Clarification des rôles et responsabilités

Afin d'assurer une sécurité adéquate, des règles de conduite et un partage des responsabilités entre les intervenants sont nécessaires. Il faut donc définir, notamment en fonction du cycle de gestion de la sécurité retenu dans l'organisation, les rôles et les responsabilités des entités impliquées dans la sécurité des actifs informationnels. Les responsabilités à l'égard de la sécurité des actifs informationnels reposent à la fois sur :

- Ceux qui en assurent la gestion;
- Les utilisateurs tant internes qu'externes au ministère ou organisme;
- Les fournisseurs de services ou les contractuels.

[5] L'Agence gouvernementale de la faune et des parcs est purement fictive. Cet exemple est inspiré de celui présenté à l'annexe 1 de la pratique recommandée intitulée « contenu type et guide à l'élaboration d'une entente de sécurité ».
[6] Document élaboré par le Secrétariat du Conseil du trésor, Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles, février 2001.

En voici quelques exemples :

Rôles	Responsabilités
Le sous-ministre	En sa qualité de premier responsable de la sécurité des actifs informationnels du Ministère, le sous-ministre : o Désigne un responsable de la sécurité de l'information numérique (RSIN); o Désigne les gestionnaires inscrits au registre d'autorité de la sécurité comme étant les détenteurs des actifs informationnels; o Approuve la politique de sécurité des actifs informationnels.
Le Comité ministériel de sécurité	Le Comité ministériel de sécurité a la responsabilité : o D'orienter, de recommander et de suivre la réalisation du plan global de sécurité du Ministère et de toute autre activité ad hoc reliée à la sécurité des actifs informationnels; o De favoriser les échanges et les relations avec les divers intervenants en gestion de la sécurité; o D'approuver les standards et les pratiques relatifs à la sécurité des actifs informationnels.
La Direction des ressources informationnelles	À titre de fournisseur de services, la Direction des ressources informationnelles a la responsabilité : o De fournir le soutien nécessaire à la mise en application de la présente politique et des directives concernant la sécurité de l'information numérique et des échanges électroniques; o De fournir les moyens et les mécanismes de sécurité pour l'application de la présente politique et d'assurer la protection des actifs informationnels ainsi que la continuité des services. Dans les régions, cette responsabilité est assumée en lien de coordination par les responsables régionaux; o D'élaborer et de faire appliquer les directives, les pratiques, standards et procédures spécifiques à leur domaine d'intervention; o D'approuver les procédures de sécurité des actifs informationnels.

7.3.4 Collecte et prise de connaissance de toute documentation utile concernant la sécurité

Il est important de collecter et de prendre connaissance de toute autre documentation disponible concernant la sécurité. Cette étape permet d'assurer l'évolution cohérente de la sécurité des actifs informationnels d'un ministère ou d'un organisme en vue de l'élaboration d'une politique de sécurité telle que définie par ce guide. Elle permet aussi de s'appuyer sur l'expérience des autres ministères et organismes en matière d'élaboration de leur propre politique de sécurité. Parmi cette documentation, on notera :

- Les orientations stratégiques;
- La politique de sécurité interne déjà existante dans l'organisation;
- Les analyses de risques et de vulnérabilités montrant les faiblesses de la sécurité des actifs informationnels;
- Le plan opérationnel de sécurité de l'organisation;
- Les directives de sécurité en vigueur;
- Les politiques de sécurité d'autres ministères ou organismes;
- Les cadres de références internationaux, normes et standards;
- Tout autre document pertinent (ex. : recommandations du Vérificateur interne).

7.4 Étape complémentaire à l'élaboration d'une politique de sécurité

7.4.1 Élaboration et maintenance du registre d'autorité de la sécurité de l'information numérique

Un registre d'autorité de la sécurité de l'information numérique doit être élaboré et adapté aux particularités de chaque ministère et organisme tel que dicté par la *Directive sur la sécurité de l'information numérique et des échanges électroniques*. Ce registre peut contenir, entre autres :

- La liste des actifs informationnels qui doivent faire l'objet de protection;
- La désignation et les attributions des détenteurs;
- La désignation et les attributions du RSIN;
- Les attributions de tout autre intervenant en matière de sécurité des actifs informationnels;
- Les noms, titres et coordonnées des personnes désignées et de leurs substituts ainsi que les dates d'entrée en vigueur de leurs attributions en matière de sécurité.

7.4.2 Inventaire des ressources

Le ministère ou organisme doit dresser un portrait de l'inventaire de ses ressources informationnelles. Ces ressources seraient constituées des actifs informationnels ainsi que des 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.

L'évaluation des ressources informationnelles existantes en termes de fonctionnalités, de stabilité, de complexité, de forces et de faiblesses permet d'analyser l'univers lié à la sécurité dans le ministère ou l'organisme concerné.

Le guide s'applique aux trois catégories d'actifs informationnels suivants :

- Ceux appartenant au ministère ou organisme et exploités par lui ;
- Ceux appartenant au ministère ou organisme et exploités par un fournisseur de services ou un tiers ;
- Ceux appartenant à un fournisseur de services ou un tiers et exploités par lui au profit du ministère ou organisme.

7.4.3 Évaluation des risques

Une évaluation des risques potentiels auxquels le ministère ou organisme est exposé doit être effectuée. Des documents identifiant plusieurs types de risque sont disponibles et peuvent être consultés dans certaines normes internationales et des standards reconnus (norme ISO/IEC TR-13335, méthode d'analyse des risques Méhari, etc.).

L'analyse des risques est une phase importante qui vient appuyer le processus d'élaboration et de révision d'une politique de sécurité. Elle permet de déterminer le niveau de risque et de vulnérabilité des ressources auquel un ministère ou un organisme est exposé et, de ce fait, constitue un outil efficace pour évaluer l'état de la sécurité d'un ministère ou organisme et préciser les priorités d'action.

7.5 Contenu type d'une politique globale de sécurité

Cette section propose un modèle de politique globale pour aider les ministères et organismes à élaborer leur propre politique globale de sécurité de l'information numérique et des échanges électroniques.

Bien que les éléments du modèle proposé ci-après soient applicables à la plupart des ministères et organismes, il convient, pour ces derniers, de les adapter à leur organisation respective et aux risques qui leur sont spécifiques.

Modèle de politique globale

Titre : Politique globale de sécurité pour le ministère (ou organisme)[7] XXXX

1.0 Introduction

1.1 Définitions

Voir lexique en annexe 1[8]

1.2 Objectifs

La politique globale de sécurité exprime la prise de position du ministère XXXX concernant les mesures de sécurité considérées comme essentielles à la protection de ses actifs informationnels. Elle regroupe les énoncés de principes généraux et les rôles et responsabilités des intervenants en sécurité du ministère.

1.3 Champs d'application

Actifs visés : Cette politique s'applique aux trois catégories d'actifs informationnels suivants :

- Ceux appartenant au ministère et exploités par lui ;
- Ceux appartenant au ministère et exploités ou détenus par un fournisseur de services ou un tiers ;
- Ceux appartenant à un fournisseur des services ou un tiers et exploités par lui au profit du ministère ou organisme.

Personnes visées : Cette politique s'adresse à tout le personnel du ministère de quelque statut qu'il soit, ainsi qu'à toute personne dûment autorisée qui a recours à l'actif informationnel du ministère dans l'exercice de ses fonctions. Les consultants, partenaires et fournisseurs utilisant et ayant accès aux biens du ministère ou ayant des biens du ministère sous leur garde, ont les mêmes obligations que le personnel du ministère.

Activités visées : Toutes les activités impliquant la manipulation ou l'utilisation sous toutes ses formes des actifs informationnels du ministère sont visées par la présente politique, que celles-ci soient conduites dans ses locaux, dans un autre lieu ou à distance.

2.0 Cadre légal et administratif

Au niveau de l'administration publique, les principales lois et directives servant de guides et de références à la politique de sécurité des actifs informationnels sont :

- Les lois d'application générale tels le Code civil, le Code criminel, la Loi concernant le cadre juridique des technologies de l'information, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, etc.;

[7] Pour les fins de ce modèle de politique globale, le terme *« ministère »* est utilisé pour désigner *« ministère ou organisme ».*
[8] Le ministère ou organisme pourra s'inspirer de l'annexe 1 du présent document pour élaborer le lexique propre à sa politique globale.

- Les lois d'application spécifique qui encadrent la mission d'un ministère. Exemple : Loi sur l'assurance hospitalisation; Loi sur les accidents de travail et les maladies professionnelles; Loi sur les régimes complémentaires de rentes, etc..

Une liste non exhaustive de lois et règlements en vigueur est présentée en annexe 4.

3.0 Énoncés de principes généraux

3.1 Protection des actifs informationnels

Cette politique globale de sécurité des actifs informationnels est fondée sur les énoncés généraux suivants :

- Les actifs informationnels du Ministère sont essentiels à ses opérations courantes et doivent faire l'objet d'une utilisation et d'une protection adéquates. Le niveau de protection accordé est fonction de leur sensibilité et des risques d'accidents, d'erreurs et de malveillance auxquels ils sont exposés

- Les gestionnaires, particulièrement ceux qui sont désignés comme détenteurs d'actifs informationnels, sont les premiers responsables de la gestion de ces actifs, de leur utilisation par les employés et de l'application des mesures de contrôle nécessaires

- La protection des actifs informationnels du ministère s'appuie sur l'implication continue de tous les gestionnaires et de tous les utilisateurs

- Chaque utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition en les utilisant avec discernement et aux seules fins prévues

3.2 Signalement des incidents

Tout utilisateur a l'obligation de signaler sans tarder au……tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité tel que vol, intrusion dans un réseau ou système, dommages délibérés, utilisation abusive, fraude, etc.

3.3 Droits de propriété intellectuelle

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

3.4 Protection des renseignements confidentiels et sensibles

Toute information considérée confidentielle ou sensible doit être protégée contre tout accès ou utilisation non autorisés ou illicites. Sont notamment confidentiels au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements nominatifs ainsi que tout renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

3.5 Continuité des activités de l'organisation

Le Ministère doit disposer de mesures d'urgence issues de son plan de continuité des services, consignées par écrit, éprouvées et mises à jour 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.).

3.6 Sensibilisation et formation

Chaque gestionnaire doit sensibiliser son personnel à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité ainsi qu'au rôle et obligations de tous les employés de son unité administrative dans le processus de protection de ces actifs. Le gestionnaire doit également veiller à ce que le personnel soit formé sur les procédures de sécurité et sur l'utilisation correcte des actifs informationnels afin de minimiser les risques de sécurité possibles.

3.7 Droit de regard

Le Ministère a un droit de regard sur l'utilisation de ses actifs informationnels par les utilisateurs. Les circonstances pour lesquelles ce droit de regard peut être exercé doivent être clairement définies et diffusées auprès des utilisateurs. Ce droit de regard sera exercé conformément à la législation notamment la Charte canadienne des droits et libertés (L.R.C. (1985) c-42), la Charte des droits et libertés de la personne du Québec (L.R.Q.,c. C-12), la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q.,c. A-2.1), la Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique et au Règlement sur l'éthique et la discipline dans la fonction publique (L.R.Q., c. F-3.1.1 a. 126, par. 1 à 3).

4.0 Rôles et responsabilités

Les rôles et responsabilités devraient être établis et complétés en fonction du cycle de gestion de la sécurité retenu dans l'organisation.

4.1 Le sous-ministre[9] (ou le dirigeant d'organisme)[10]

Il est le premier responsable des actifs informationnels du Ministère. Il approuve la présente politique.

4.2 Le responsable de la sécurité de l'information numérique (RSIN)[11]

En conformité avec la *Directive sur la sécurité de l'information numérique et des échanges électroniques*, le responsable de la sécurité de l'information numérique (RSIN) agit à titre de représentant désigné par le sous-ministre ou le dirigeant d'organisme pour coordonner la sécurité de l'information du Ministère. À cet effet, il a la responsabilité, entre autres :

- De proposer les orientations de sécurité de l'information et les communiquer au personnel ainsi qu'aux partenaires du Ministère;
- D'élaborer et d'assurer le suivi et la mise à jour périodique du plan de sécurité de l'information;
- D'assurer la coordination des grands projets de sécurité;
- De faire rapport au comité de sécurité du Ministère et lui rendre compte de l'état d'avancement des dossiers de sécurité des actifs informationnels.

[9] Les attributions du sous-ministre ou dirigeant de l'organisme sont listées dans la *« Directive sur la sécurité de l'information numérique et des échanges électroniques »*
[10] Selon le contexte propre à l'organisation, on choisira les termes *« sous-ministre »* ou *« dirigeant d'organisme »*
[11] Les attributions du RSIN sont listées dans la *« Directive sur la sécurité de l'information numérique et des échanges électroniques »*

4.3 Le comité sur la sécurité de l'information numérique

Agit à titre de mécanisme de coordination et de concertation de la sécurité de l'information. Ce comité recommande les orientations et les directives au sous-ministre et approuve les standards, les pratiques et le plan d'action de sécurité des actifs informationnels du ministère.

4.4 Le responsable de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

Veille au respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels au sein du Ministère et plus particulièrement dans le cadre du développement de systèmes d'information.

4.5 Le détenteur de l'information numérique

Agit à titre de responsable désigné de la protection d'un actif informationnel. À cet effet, il :

- Assure la gestion de la sécurité de son actif informationnel;
- Veille à ce que les mesures de sécurité appropriées soient élaborées, mises en place et appliquées;
- Participe à la sensibilisation des utilisateurs aux besoins de sécurité de l'information qu'ils manipulent;
- Répond de l'utilisation, par les utilisateurs et les partenaires du Ministère, des données dont il est le détenteur. À cet égard, il voit à élaborer un protocole d'entente avec les entités utilisatrices et à le faire respecter.

4.6 Le responsable de la sécurité physique et matérielle

Le responsable de la sécurité physique et matérielle agit à titre de gestionnaire de la sécurité physique des lieux et des personnes. Il est responsable du contrôle d'accès physique aux immeubles du Ministère, de même que du contrôle de la circulation des équipements informatiques sortant des immeubles.

4.7 Le gestionnaire

Les principales responsabilités du gestionnaire à l'égard de la protection des actifs informationnels sont, entre autres :

- D'informer et sensibiliser son personnel quant aux dispositions de la présente politique et des modalités liées à sa mise en œuvre;
- De s'assurer que les ressources informationnelles sont utilisées en conformité avec les principes généraux et les autres exigences de la présente politique;
- De répondre de l'utilisation faite par son personnel des actifs informationnels du Ministère;

4.8 L'utilisateur

L'utilisateur d'un actif informationnel :

- Prend connaissance et adhère à la politique de sécurité des actifs informationnels;
- Utilise les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont autorisés;
- Se conforme aux consignes et directives établies et dans le respect des dispositions de la présente politique.

4.9 La Direction des ressources informationnelles

Assure la mise en application des exigences de sécurité des actifs informationnels du Ministère durant tout le cycle de vie de l'information numérique. Ses principales responsabilités sont, entre autres :

- D'assurer la sécurité des actifs informationnels relevant de sa responsabilité;
- D'assurer la disponibilité, l'intégrité, la confidentialité, l'authentification, l'irrévocabilité de l'information numérique selon les exigences et les droits d'accès définis par les détenteurs des actifs informationnels;
- De fournir aux détenteurs le soutien et les conseils en matière de protection de leurs actifs informationnels;
- De restreindre les accès de son personnel spécialisé en technologies de l'information, notamment les administrateurs de réseaux, aux seules informations indispensables à l'exercice de leurs fonctions.
- D'approuver les procédures et de voir à l'application des directives, pratiques et standards.

4.10 La Direction de la vérification interne

Effectue des examens de conformité indépendants et objectifs de l'efficacité des contrôles qui s'inscrivent dans les activités de la protection des actifs informationnels du Ministère et ce, dans un contexte de gestion intégrée des risques. Elle s'associe au processus de bilan annuel de sécurité afin d'en assurer la conformité.

5.0 Dispositions finales

5.1 Sanctions

Lorsqu'un utilisateur d'actif informationnel contrevient à cette politique ou aux directives internes en découlant, le sous-ministre détermine, selon la nature ou la gravité du cas, de l'opportunité d'appliquer une sanction disciplinaire ou une mesure administrative qui peut inclure une réprimande, une suspension ou un congédiement et ce, conformément aux dispositions des conventions collectives ou ententes. La révocation de l'utilisation d'actifs informationnels peut également être envisagée.

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

5.2 Révision

Afin d'assurer son adéquation aux besoins de sécurité du ministère, la présente politique doit être régulièrement révisée et, au plus tard, trois années après sa mise en application ainsi que lors de changements qui pourraient l'affecter.

5.3 Mise en application et suivi de la politique

Le responsable nommé par le sous-ministre ou le dirigeant d'organisme est chargé de l'application de la présente politique.

5.4 Date d'entrée en vigueur

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

5.5 Approbation

La présente politique de sécurité des actifs informationnels est approuvée par _____, le _____.

7.6 Contenu type d'une directive de sécurité

Comme précisé dans la section 7.2.2 ci-dessus, l'objectif d'une directive de sécurité est de permettre aux ministères et organismes d'identifier les mesures de sécurité nécessaires à la protection de leurs actifs informationnels.

Un modèle de contenu type d'une (ou des) directive (s) de sécurité est proposé à l'annexe 5. Ce modèle s'appuie sur la norme ISO 17799 et en suit l'arborescence des sections. Il fournit un ensemble de mesures de sécurité lesquelles ne seront pas toutes applicables à chaque ministère et organisme qui ne retiendra que celles répondant au mieux à ses préoccupations de sécurité des actifs informationnels.

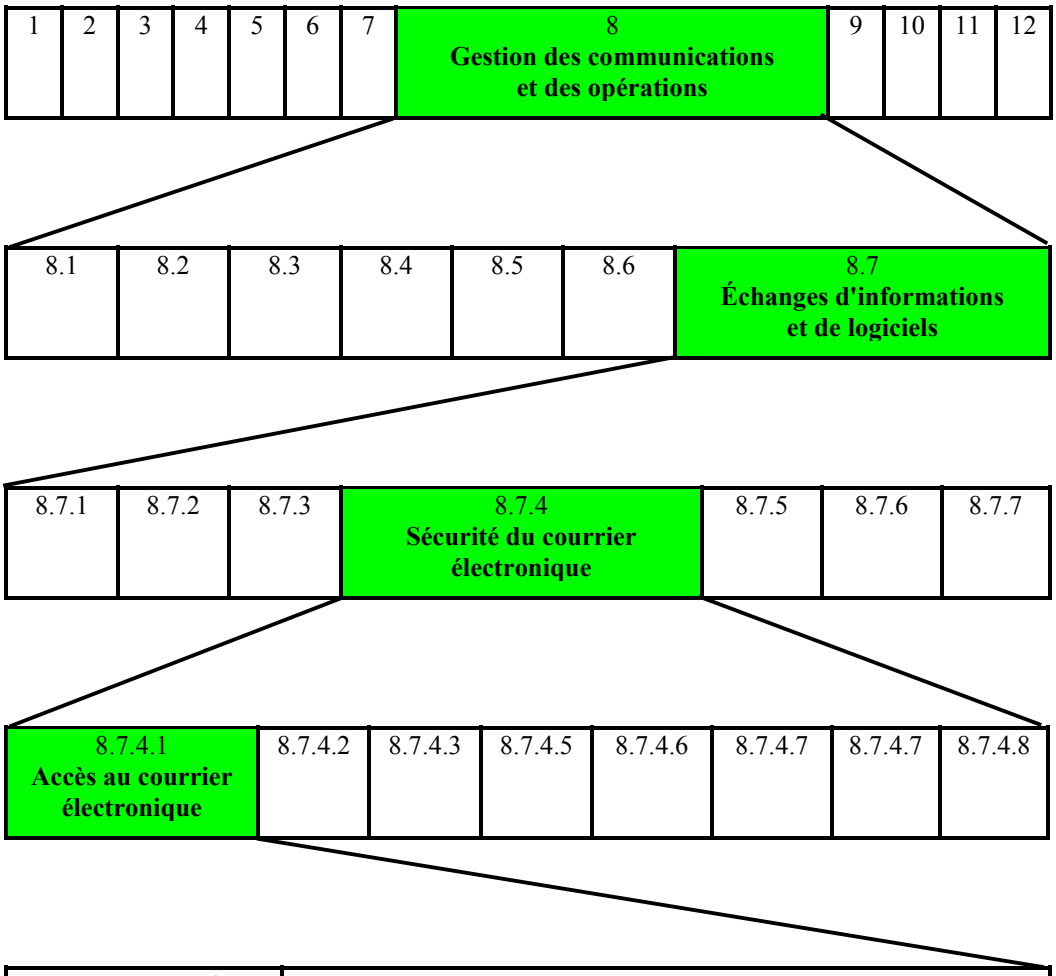
Les grandes sections du modèle de directive(s) sont subdivisées en sous-sections jusqu'à un maximum de trois (3) niveaux. Le dernier niveau étant celui qui, généralement, liste les mesures de sécurité des actifs informationnels. Dans certains cas, il pourrait s'avérer nécessaire d'aller au-delà du troisième niveau en éclatant ce dernier en mesures plus fines. La section suivante propose un canevas pour identifier l'ensemble des mesures et en assurer une description détaillée.

L'utilisation de ce canevas apporte une valeur ajoutée qui se traduit par les deux éléments suivants :

- ✓ Association des risques aux mesures de sécurité énoncées;
- ✓ Structure des liens qui en facilitent la publication et la gestion sur des sites Web intranet ou extranet.

7.6.1 Modèle d'élaboration de directive(s) de sécurité selon la norme ISO 17799

La figure suivante propose un canevas pour énoncer une mesure relative à une directive de sécurité. Elle présente un cas où il s'est avéré nécessaire de se rendre au quatrième niveau du modèle pour préciser la directive et fournit l'information requise pour permettre aux utilisateurs de comprendre et d'appliquer sans délais la mesure de sécurité concernée. Ce canevas, relatif à la section 8 de la norme ISO 17799, s'applique à tous les éléments présentés à l'annexe 5 indépendamment du niveau auquel on s'arrête.



Mesures de sécurité	Les employés et les sous–traitants du ministère ou organisme doivent employer des comptes de courrier électronique approuvés par le ministère ou organisme
Note explicatives	L'information relevant de la responsabilité du ministère ou organisme doit être échangée par l'intermédiaire des comptes de courrier électronique fournis ou approuvés par ce ministère ou organisme. À ce titre, les systèmes de courrier électronique publics tels que Hotmail, Yahoo, etc… ne doivent pas être utilisés.
Risques de sécurité	Les systèmes de courrier électronique publics augmentent les risques de divulgation de l'information sensible à des personnes non autorisées avec, pour conséquence, la perte de confiance de la clientèle
Références	• Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique • Directive sur l'utilisation d'Internet

7.6.2 Corrélation entre les énoncés de la norme ISO/IEC 17799 et l'AGSIN

La subdivision des éléments à considérer pour la sécurisation des actifs informationnels permet une meilleure prise en charge de la sécurité. Cette approche est, entre autres, utilisée par :

- La norme ISO/IEC 17799 qui propose un regroupement par domaine de sécurité (exemple : organisation de la sécurité, sécurité du personnel, sécurité physique et sécurité de l'environnement, classification de l'information et contrôle des actifs, etc.);

- L'AGSIN qui regroupe, selon différentes dimensions de la sécurité, les éléments à considérer par les intervenants en sécurité des actifs informationnels dans les ministères et organismes (M/O). Un extrait de l'AGSIN, joint à l'annexe 3, donne une répartition des éléments de sécurité particuliers à chacune des dimensions : juridique, humaine, organisationnelle et technologique.

Tel que mentionné précédemment, le présent guide propose, dans la structuration du contenu type d'une directive de sécurité, le regroupement des éléments de sécurité selon la norme ISO/IEC 17799.

Le tableau proposé ci-après assure la corrélation entre les énoncés de la norme ISO/IEC 17799 et l'AGSIN. La section de couleur noire (première et deuxième colonne) de ce tableau reprend les divisions de l'AGSIN. La section de couleur gris clair (colonne de droite) repose sur la norme ISO/IEC 17799.

Dimension de la sécurité provenant de l'AGSIN	***Sous-dimension de la sécurité provenant de l'AGSIN***	***Énoncés de la norme ISO/IEC 17799***
Dimension juridique	Aspects légaux	➢ 8.7 Échanges d'information et de logiciels ➢ 12.1 Conformité aux exigences légales
Dimension humaine	Sécurité appliquée au personnel	➢ 6.1 Sécurité dans la définition des postes et des ressources ➢ 6.2 Formation des utilisateurs ➢ 6.3 Réactions aux incidents de sécurité et aux défauts de fonctionnement
	Éthique, pratique professionnelle et imputabilité	➢ 6.1 Sécurité dans la définition des postes et des ressources ➢ 6.3 Réactions aux incidents de sécurité et aux défauts de fonctionnement ➢ 9.3 Responsabilités des utilisateurs ➢ 10.5 Sécurité des environnements de développement et de soutien

Dimension de la sécurité provenant de l'AGSIN	***Sous-dimension de la sécurité provenant de l'AGSIN***	***Énoncés de la norme ISO/IEC 17799***
Dimension organisationnelle	Sécurité administrative	➢ 3.1 Politique de sécurité de l'information ➢ 4.1 Infrastructure de la sécurité de l'information ➢ 4.2 Sécurité des accès par des tiers ➢ 4.3 Sous-traitance ➢ 5.1 Responsabilités liées aux actifs ➢ 5.2 Classification de l'information ➢ 7.3 Mesures générales ➢ 8.1 Procédures et responsabilités opérationnelles ➢ 8.4 Intendance ➢ 8.5 Gestion des réseaux ➢ 8.6 Manipulation et sécurité des supports ➢ 8.7 Échanges d'information et de logiciels ➢ 9.2 Gestion des accès utilisateurs ➢ 9.4 Contrôle de l'accès aux réseaux ➢ 9.8 Informatique mobile et télétravail ➢ 11.1 Aspects de la gestion de la continuité des activités de l'organisation ➢ 12.2 Examens de la politique de sécurité et de la conformité technique
	Sécurité physique et du milieu	➢ 7.1 Zones de sécurité ➢ 7.2 Sécurité du matériel ➢ 7.3 Mesures générales ➢ 8.5 Gestion des réseaux ➢ 8.6 Manipulation et sécurité des supports ➢ 9.1 Exigences de l'organisation concernant le contrôle des accès ➢ 9.2 Gestion des accès utilisateurs ➢ 9.4 Contrôle de l'accès aux réseaux ➢ 10.4 Sécurité des fichiers ➢ 10.5 Sécurité des environnements de développement et de soutien
	Sécurité des opérations	➢ 4.2 Sécurité des accès par des tiers ➢ 8.5 Gestion des réseaux ➢ 8.6 Manipulation et sécurité des supports ➢ 9.1 Exigences de l'organisation concernant le contrôle des accès ➢ 9.2 Gestion des accès utilisateurs ➢ 9.4 Contrôle de l'accès aux réseaux ➢ 9.5 Contrôle de l'accès aux systèmes d'exploitation ➢ 9.6 Contrôle de l'accès aux applications ➢ 9.7 Surveillance des accès aux systèmes et de leur utilisation ➢ 10.2 Sécurité des systèmes d'application ➢ 10.4 Sécurité des fichiers ➢ 10.5 Sécurité des environnements de développement et de soutien ➢ 11.1 Aspects de la gestion de la continuité des activités de l'organisation ➢ 12.3 Considérations sur les audits des systèmes

Dimension de la sécurité provenant de l'AGSIN	*Sous-dimension de la sécurité provenant de l'AGSIN*	*Énoncés de la norme ISO/IEC 17799*
Dimension technologique	Sécurité des logiciels, du matériel, des communications et des informations de sécurité	➢ 7.2 Sécurité du matériel ➢ 7.3 Mesures générales ➢ 8.2 Planification et recette des systèmes ➢ 8.3 Protection contre les logiciels pernicieux ➢ 8.4 Intendance ➢ 8.5 Gestion des réseaux ➢ 8.6 Manipulation et sécurité des supports ➢ 8.7 Échanges d'informations et de logiciels ➢ 9.4 Contrôle de l'accès aux réseaux ➢ 9.5 Contrôle de l'accès aux systèmes d'exploitation ➢ 9.6 Contrôle de l'accès aux applications ➢ 9.8 Informatique mobile et télétravail ➢ 10.1 Exigences de sécurité des systèmes ➢ 10.2 Sécurité des systèmes d'applications ➢ 10.3 Mesures cryptographiques ➢ 10.4 Sécurité des fichiers ➢ 10.5 Sécurité des environnements de développement et de soutien ➢ 12.3 Considérations sur les audits des systèmes

7.7 Plan de validation de la politique

L'expérience vécue par certains ministères et organismes concernant l'étape de validation d'une politique de sécurité démontre que cette étape peut être longue selon l'envergure du ministère et organisme, de sa structure organisationnelle et la diversité des intervenants tel que présenté à la section 6. La prise en compte de ces éléments a une incidence directe sur les délais de validation qui peuvent représenter une proportion allant de un à six fois le temps pris pour l'élaboration de la politique elle-même.

L'étape de validation est avantageusement appuyée par un plan de validation dont l'exécution peut se faire selon plusieurs étapes. Chacune de ces étapes donnera lieu à un état de validation dans lequel seront consignées les informations suivantes :

- Nom de la personne responsable de la validation ainsi que son unité d'appartenance;
- Commentaires reçus.

À titre d'exemple, les étapes d'un plan de validation d'une politique globale de sécurité d'un ministère pourraient être :

- **Étape 1** : Validation par le personnel professionnel et technique de la Direction du soutien aux technologies de l'information;
- **Étape 2** : Validation par les directions du ministère ou de l'organisme concerné;
- **Étape 3** : Validation par les comités internes au ministère et organisme;
- **Étape 4** : Validation par les directeurs généraux et les sous-ministres.

Les ministères et organismes pourront adapter les étapes de validation à leur structure organisationnelle et selon la composante de politique à valider. Ainsi, les quatre étapes précédentes s'appliqueront à la validation d'une politique globale ou d'une directive alors que la validation d'une pratique, d'un standard ou d'une procédure nécessiteront, du fait de leur caractère technique, des niveaux d'intervention différents.

7.8 Mise en œuvre, diffusion et gestion de la politique de sécurité

La mise en œuvre de la politique de sécurité d'un ministère ou organisme est une étape cruciale. Le caractère opérationnel de la politique de sécurité amène des obligations et, parfois même, des modifications organisationnelles importantes. La mise en application ordonnée des mesures énoncées dans les composantes de celle-ci (politique globale, directives, pratiques, standards et procédures) s'impose.

À cet égard, la constitution d'un projet de déploiement de ces composantes, en tout ou en partie, et la désignation d'une équipe responsable de cette tâche s'avère un gage de succès.

À cette étape-ci, on établira également les grandes bases des stratégies du plan de communication et de gestion de la politique.

La mise en œuvre d'une composante ou d'un de ses éléments peut être envisagée dès son approbation sans pour autant attendre que toutes les composantes soient réalisées. À titre d'exemple :

- ✓ une directive sur la sécurité du courrier électronique peut être mise en œuvre indépendamment de l'avancement des autres directives de sécurité ou des procédures de déploiement des logiciels antivirus;
- ✓ une pratique sur le plan de sauvegarde des informations peut être mise en œuvre indépendamment de la disponibilité d'une pratique sur le plan de relève ou d'une directive qui en fait obligation.

7.8.1 Plan de communication de la politique de sécurité

Le plan de communication de la politique de sécurité consiste à assurer la propagation de celle-ci à l'ensemble du personnel du ministère ou organisme. Ce plan vise notamment à :

- ✓ Former et sensibiliser le personnel à l'importance de la sécurité des actifs informationnels et au respect de la politique de sécurité;
- ✓ S'assurer de la prise en charge des rôles et responsabilités dévolus aux intervenants;
- ✓ Mettre en place les outils de soutien appropriés.

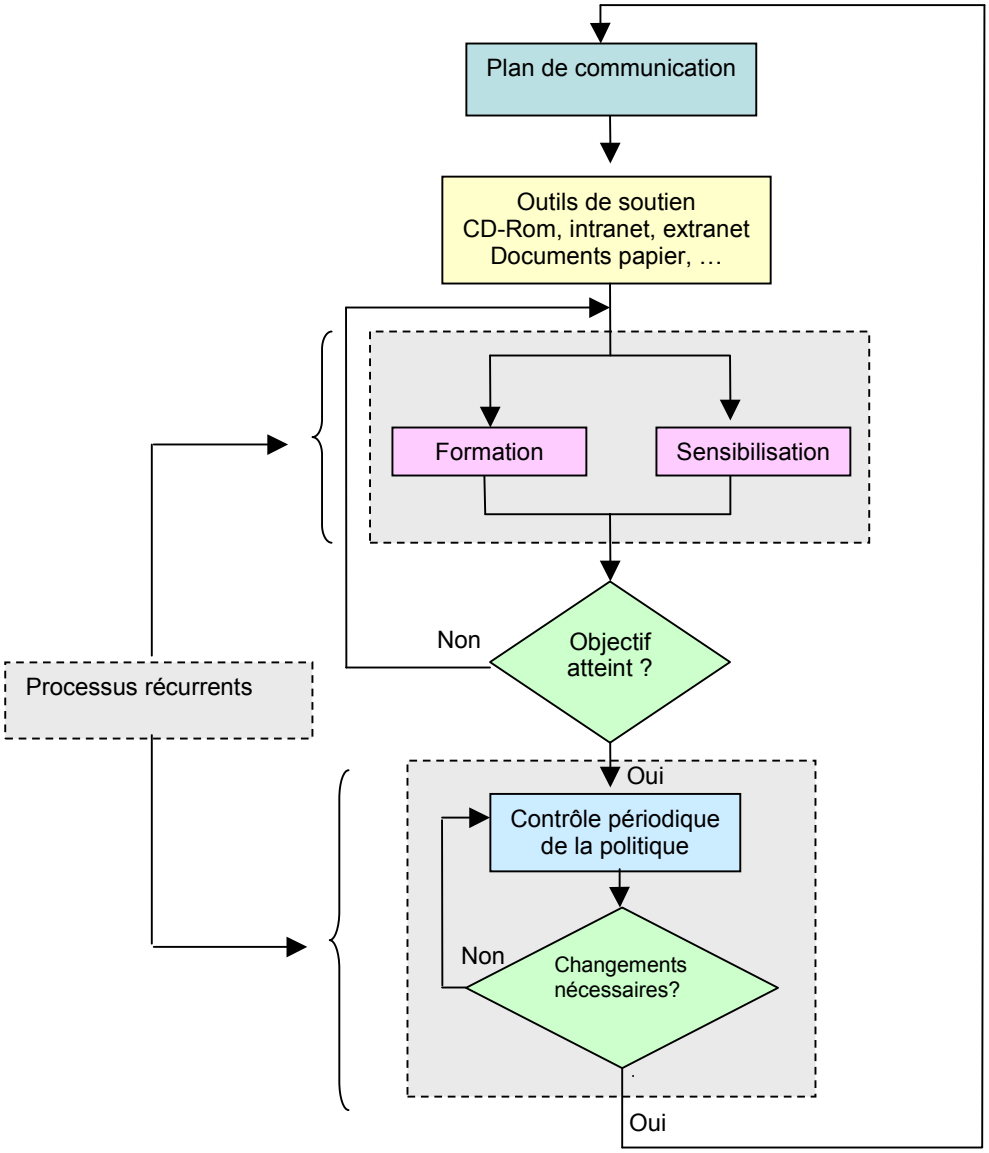
Une méthode ordonnée de diffusion de la politique de sécurité doit être suivie afin de rejoindre tous les employés et de s'assurer que chacun comprend et accepte ses responsabilités quant à cette politique.

La lettre de déclenchement du processus de diffusion de la politique de sécurité doit émaner de la plus haute autorité du ministère ou de l'organisme. Cette lettre devrait démontrer le soutien et l'engagement de la haute direction en ce qui concerne la sécurité de l'information dans toute l'organisation.

De plus, la lettre devrait confirmer l'adhésion de la haute direction aux principes de contrôle et d'évaluation réguliers de la sécurité des actifs informationnels et confier aux gestionnaires la responsabilité du suivi du déploiement de la politique de sécurité lors des différents comités de gestion du ministère ou organisme.

Le schéma suivant illustre le processus de communication de la politique de sécurité au sein de l'organisation :

Processus de communication de la politique de sécurité au sein de l'organisation



Note : les éventuels changements nécessaires à la politique de sécurité peuvent entraîner une mise à jour du plan de communication et des outils de soutien. Ils peuvent également enclencher de nouvelles actions de formation et de sensibilisation.

Les outils susceptibles de soutenir la communication de la politique de sécurité à l'ensemble du personnel de l'organisation sont diversifiés. Parmi ceux-ci, on retrouve :

- ✓ Bannières publicitaires sur le site intranet ou extranet de l'organisation;
- ✓ Articles dans les journaux internes;
- ✓ Sites Web (intranet ou extranet);
- ➢ Documents situés sur un serveur commun;
- ✓ Documents distribués au personnel;
- ✓ Trousses de sensibilisation à la sécurité;
- ✓ Séances d'information et de formation;
- ✓ Information spécifique aux nouveaux employés lors des séances d'accueil;
- ✓ Etc.

Les mesures du taux de pénétration de la politique et de la prise de conscience du personnel concernant la sécurité des actifs informationnels constituent des facteurs de succès de la communication de la politique. Parmi les moyens généralement mis en place pour assurer ces mesures, on retrouve :

- ✓ Les listes de distribution de courriels;
- ✓ Les feuilles de présences aux séances de formation, de sensibilisation ou d'information;
- ✓ L'identification des usagers accédant à une formation en ligne;
- ✓ Etc.

La politique de sécurité est un élément évolutif. La mise en place d'un mécanisme permettant d'informer le personnel de tout changement y afférent devient nécessaire. Divers moyens de propagation des modifications peuvent être utilisés :

- ✓ Distribution de communiqués;
- ✓ Envoi de courriels;
- ✓ Tenue de réunions;
- ✓ Parution d'une annonce sur le site intranet du ministère ou organisme;
- ✓ Journal Internet;
- ✓ Etc.

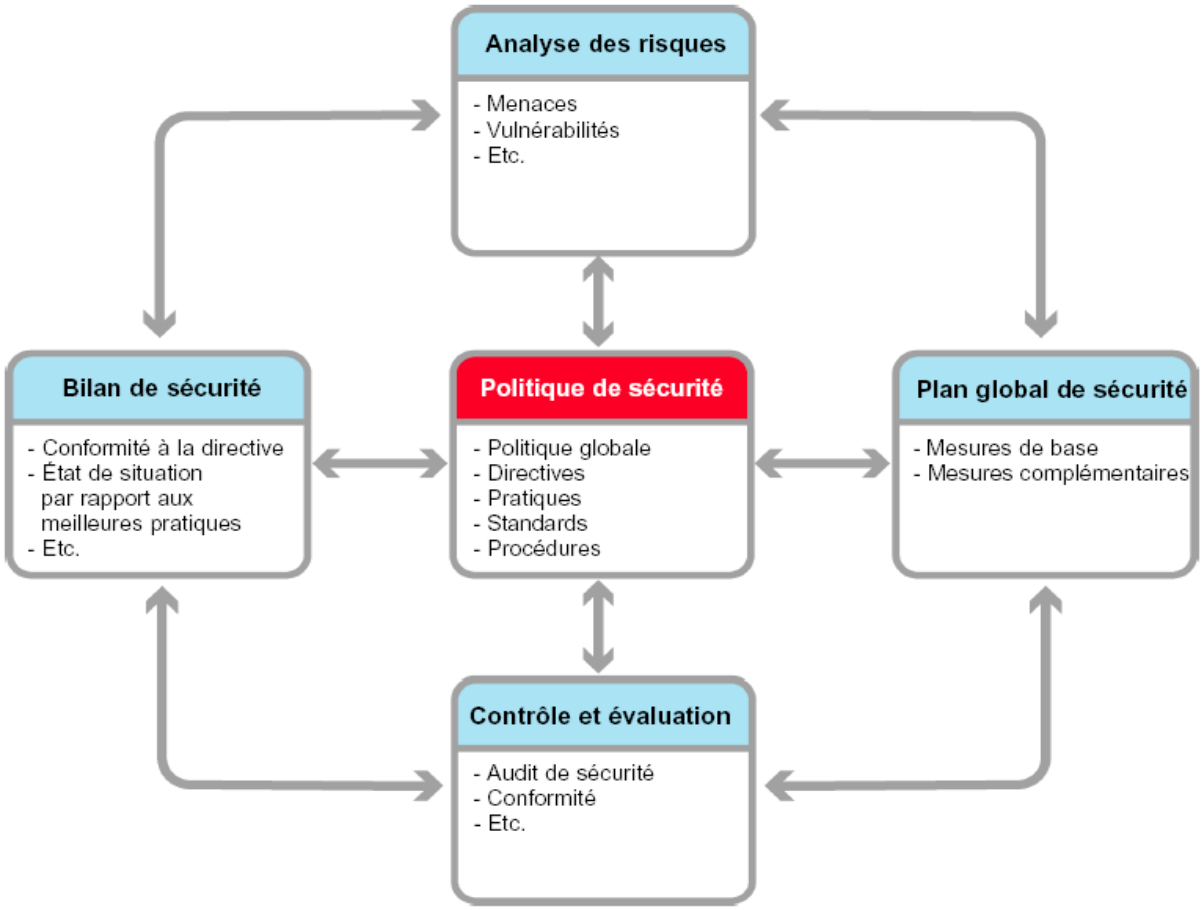
7.8.2 Gestion de la politique de sécurité

7.8.2.1 Révision de la politique

Afin d'assurer son adéquation aux besoins de sécurité du ministère ou organisme, le contenu d'une politique de sécurité doit être régulièrement révisé et, au plus tard, trois années après sa mise en application ainsi que lors de changements qui pourraient l'affecter.

En effet, l'apparition de nouvelles menaces et vulnérabilités, l'évolution constante de l'environnement technologique et des façons de faire sont des exemples non exhaustifs d'évènements susceptibles d'affecter, partiellement ou en totalité, le caractère opérationnel d'une politique de sécurité.

À cet égard, les évènements déclencheurs d'une révision de la politique sont repris dans le schéma ci-après. Il est à noter que ces mêmes éléments constituent les principales composantes du modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise (voir schéma joint en annexe 2).



7.8.2.2 Facteurs clés de succès d'une politique de sécurité

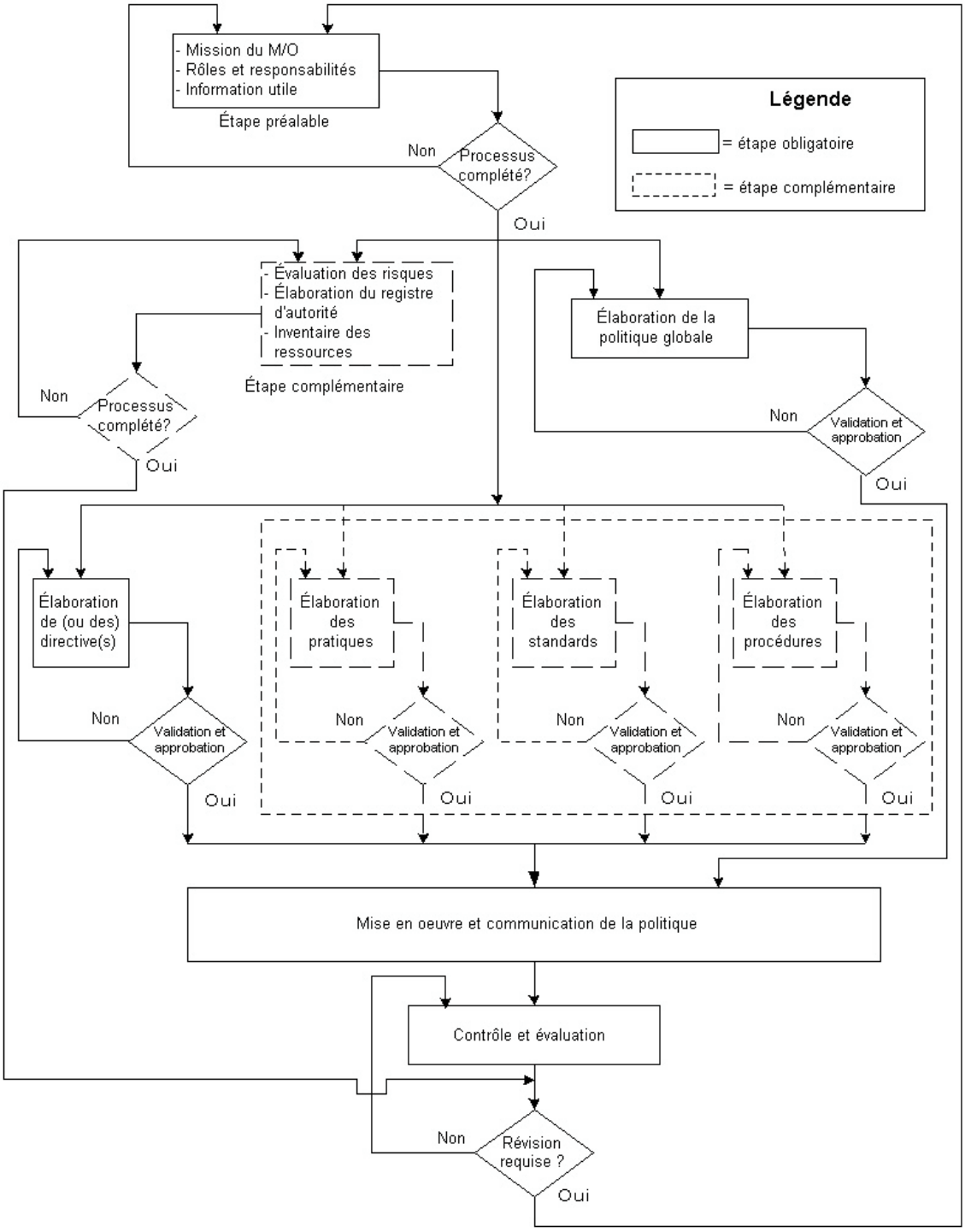
Les facteurs clés de succès traduisent la liste des actions les plus importantes à réaliser afin que la politique de sécurité atteigne ses objectifs. Ils s'adressent à l'ensemble du personnel, y compris la haute direction et les gestionnaires, et permettent de rencontrer les objectifs de mise en œuvre de la politique de sécurité au sein du ministère ou organisme. Ils se traduisent par les principales actions suivantes :

- Les énoncés de missions, les objectifs stratégiques, les orientations de la politique globale et les mesures émanant de directives de sécurité sont bien définis et clairement formulés;
- Un programme de sensibilisation et de formation du personnel aux énoncés de la politique et à la sécurité des actifs informationnels est mis en place;
- Une assistance concrète, pour la mise en pratique des éléments constituants de la politique est mise en place;
- Un processus d'évaluation pour mesurer le niveau de sensibilisation et le respect de la politique adoptée est mis en place;
- La haute direction et le personnel ont une vision commune des exigences de sécurité, des points faibles et des menaces et ils comprennent et acceptent leurs propres responsabilités dans ce domaine;
- La haute direction souscrit aux principes de contrôle et d'évaluation (audit indépendant) de la sécurité de façon régulière et s'y implique;
- La politique de sécurité est périodiquement évaluée;
- Les détenteurs des actifs informationnels sont précisés;
- La politique globale de sécurité est appuyée par des processus (processus de gestion et d'évaluation des risques, de continuité des services, de gestion des incidents, etc.), des directives et des pratiques

7.9 Processus d'élaboration, de mise en œuvre et de gestion d'une politique de sécurité des actifs informationnels

Le tableau suivant reprend, sous forme graphique, le cheminement présenté dans la section 7.

.


- Mission du M/O
- Rôles et responsabilités
- Information utile
Étape préalable
Non
Processus complété?
Oui
Légende
= étape obligatoire
= étape complémentaire
- Évaluation des risques
- Élaboration du registre d'autorité
- Inventaire des ressources
Étape complémentaire
Élaboration de la politique globale
Non
Processus complété?
Oui
Non
Validation et approbation
Oui
Élaboration de (ou des) directive(s)
Élaboration des pratiques
Élaboration des standards
Élaboration des procédures
Non
Validation et approbation
Oui
Mise en oeuvre et communication de la politique
Contrôle et évaluation
Non
Révision requise ?
Oui

8. Conclusion

Le cadre de référence d'une politique de sécurité, élaboré dans le présent guide, vise l'atteinte des objectifs de sécurité précisés dans la *Directive sur la sécurité de l'information numérique et des échanges électroniques* et le respect des fonctions développées dans l'AGSIN. Particulièrement, il propose aux ministères et organismes :

- ✓ Une démarche visant à faciliter la réalisation des travaux requis par l'activité de mise en place et de gestion d'une politique de sécurité;
- ✓ Un modèle structuré d'une politique de sécurité;
- ✓ Des contenus types des principales composantes de cette politique (politique globale, directive(s));
- ✓ Des procédés de mise en œuvre, de communication et de gestion inspirés de la réalité gouvernementale.

Ce guide s'inspire du projet de norme ISO/IEC-17799, en cours d'officialisation. Ce choix permet aux ministères et organismes de s'appuyer sur un code de bonnes pratiques internationalement reconnu, de se placer à l'avant-garde en matière de sécurité des actifs informationnels et de s'adapter rapidement aux améliorations qui surviendront à cette norme, point de convergence des meilleures pratiques. De plus, la structure proposée par cette norme facilite l'utilisation d'outils électroniques de type Web pour élaborer, gérer et communiquer la politique de sécurité.

9. Références

- Lois générales, directives, règlements, normes, guides et standards (voir annexe 4)

- CoBit, 3ème édition, Association française de l'audit (AFAI) & IT Governance Institute.

- Gouvernement du Québec, Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles, Direction de l'architecture et de l'infrastructure. Quelques définitions utiles sur la normalisation, 22 avril 2002.

- Gouvernement du Québec, Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles, Direction de l'architecture et de l'infrastructure, Quatre catégories de standards au gouvernement du Québec, 5 février 2002.

- Québec (Province), Ministère des Ressources naturelles, Politique de sécurité de l'information électronique et des actifs informationnels, 18 juin 1998.

- Québec (Province), Ministère des Ressources naturelles, Politique d'utilisation des services de l'inforoute, 25 octobre 1999.

- Québec (Province), ministère de l'Industrie et du commerce, Politique de sécurité de l'information et des échanges électroniques, 5 mars 2002.

- Québec (Province), Société de l'assurance automobile du Québec, Politique sur la sécurité informatique, 1er février 2000.

- Québec (Province), Ministère des Relations avec les citoyens et de l'Immigration, Document de travail intitulé *« Politique ministérielle de la sécurité de l'information numérique et des échanges électroniques »*, 20 décembre 2002.

- Québec (Province), Ministère des relations avec les citoyens et de l'Immigration, Document de travail intitulé *« Orientation et organisation de la documentation de la sécurité de l'information numérique et des échanges électroniques »*, 25 novembre 2002.

- Québec (Province), Régie de l'assurance maladie, Document de travail intitulé *« Sécurité de l'information – Politique générale »*, 27 janvier 2003.

- Québec (Province), Régie de l'assurance maladie, Document de travail intitulé *« Gestion de la sécurité de l'information – Politique administrative »*, 27 janvier 2003.

- Québec (Province), Régie de l'assurance maladie, Document de travail intitulé *« Sécurité physique des actifs informationnels – Politique administrative »*, 27 janvier 2003.

- Québec (Province), Ministère de la Sécurité publique, Document de travail intitulé *« Politique ministérielle de la sécurité de l'information numérique et des échanges électroniques »*.

- Grand dictionnaire terminologique. Office québécois de la langue française.

Annexes

Annexe 1 : Lexique

a) Abréviations

« AGSIN » : *Architecture gouvernementale de la sécurité de l'information numérique.*

« ASIN » : *Architecture de sécurité de l'information numérique.*

« DICAI » : *Disponibilité, intégrité, confidentialité, authentification, irrévocabilité.*

« RSIN » : *Responsable de la sécurité de l'information numérique.*

« SSIGRI » : *Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles.*

b) Définitions

« Actif informationnel » *: Une information numérique, une banque d'information numérique, 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 une organisation.*

« Administration » : *Fonction permettant de gérer les processus et outils de sécurité entourant les équipements, les logiciels et les réseaux.*

« Analyse et évaluation des risques » : *Analyse et évaluation des menaces, des impacts et des vulnérabilités auxquels l'information et les infrastructures de traitement de l'information sont exposés et de la probabilité de leur survenance.*

« Application » : *Ensemble organisé de moyens informatiques (traitements, données et interfaces), incluant les progiciels, mis en place pour recueillir, traiter, emmagasiner, communiquer et éliminer l'information dans le but de répondre à un besoin déterminé et de supporter les processus de travail des utilisateurs.*

« Authentification » : *Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.*

« Banque d'information » : *Collection d'information relative à un domaine défini, regroupée et organisée de façon à en permettre l'accès.*

« Chiffrement » : *Opération par laquelle est substitué à un texte en clair, un texte inintelligible pour quiconque ne possédant pas la clé permettant de le ramener à sa forme initiale.*

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

« Confidentialité » : *Propriété d'une information de n'être accessible qu'aux personnes autorisées.*

« Continuité» : *Propriété qu'ont les ressources informationnelles d'être accessibles de la manière requise (sans interruption, délai ou dégradation) et utilisables au moment voulu.*

« Contrôle d'accès » *: Fonction permettant aux systèmes de contrôler l'accès aux ressources selon des autorisations préalablement définies par la fonction habilitation.*

« Courriel » : *Service de correspondance sous forme d'échange de messages électroniques à travers un réseau de télécommunications.*

« Cycle de vie de l'information numérique» : *Période de temps couvrant toutes les étapes d'existence de l'information numérique dont celles de la définition, de la création, de l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction de cette information.*

« Détenteur » : *Gestionnaire à qui est assignée la responsabilité de la sécurité d'un actif informationnel et / ou d'un processus d'affaires.*

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

« Document technologique » : *Information délimitée et structurée de façon logique sur un support faisant appel aux technologies de l'information, intelligible sous forme de mots, de sons ou d'images. Est assimilée au document technologique toute banque de données dont les éléments structurants permettent la création de documents par la délimitation ou la structuration de l'information qui y est inscrite*[12].

« Équipements informatiques » : *Tout équipement de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception, et de traitement de l'information et tout équipement de télécommunication.*

« Fichier » : *Collection d'information consignée et stockée comme une entité unique et spécifique sur un support de stockage.*

« Fournisseur » : *Organisme privé ou public ou personne physique qui fait affaire avec un ministère ou organisme en vue de lui fournir des services ou des biens informatiques.*
Notes:
1. *Exemples d'organisme privé: corporation, société, coopérative.*
2. *Exemples d'organisme public: tout fonds spécial du gouvernement du Québec.*

« Gestion des risques en sécurité » : *Processus d'identification, de contrôle et de réduction ou d'élimination des risques de sécurité qui pourraient affecter les actifs informationnels, moyennant un coût acceptable.*

« Habilitation » : *Fonction permettant d'attribuer à un utilisateur l'autorisation de porter des actions sur les ressources.*

[12] Articles 1(2°) et 3 de la Loi concernant le cadre juridique des technologies de l'information.

« Information numérique » : *Information dont l'usage n'est possible qu'au moyen de technologies de l'information.*

« Inforoute » : *Réseau étendu d'information à haut débit et à grande vitesse, capable de transmettre des données de toutes sortes, notamment des données multimédias, et destiné à jouer le rôle d'infrastructure globale de communication au service de l'ensemble des populations, sur les plans national et international.*

«Infrastructure commune » *: Ensemble des composantes matérielles, logicielles, technologiques et organisationnelles ainsi que les services communs y compris l'expertise technique utilisés en tout ou partie par plusieurs ministères et organismes.*

« Intégrité » : *Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation.*

Note :
1. L'intégrité fait référence à l'exactitude ou à l'état complet de l'information.

« Internet » : *Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés qui sont reliés par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique de communication à leurs utilisateurs.*

« Irrévocabilité » : *Propriété d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.*

« Logiciel » : *Ensemble commercialisé de programmes et procédés relatifs au traitement informatique des données.*

« Mesure de sécurité » : *Moyen organisationnel, technologique, humain ou juridique permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.*

« Mot de passe » : *Authentifiant prenant la forme d'une chaîne de caractères, d'un code secret choisi par l'utilisateur, que celui-ci doit entrer lors de la procédure d'accès à un système informatique, notamment à un réseau ou à sa boîte aux lettres électronique.*

« Norme » : *Accord documenté 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.*

Note :
1. Le terme « norme » accompagné du qualificatif « internationale » , « nationale » ou « européenne » signifie une norme reconnue par un organisme officiel.

« Politique de sécurité de l'information numérique » : *Ensemble de documents produits constitués de la politique globale, des directives, des standards, des pratiques et des procédures qui régissent les exigences d'un ministère ou organisme en matière de sécurité de l'information numérique.*

« 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.*

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

« Registre d'autorité de la sécurité de l'information numérique » *: Recueil où sont inscrites les désignations de personnes affectées à des responsabilités particulières concernant la gestion de la sécurité de l'information numérique.*

« Renseignement de nature confidentielle » : *Renseignement qui ne doit pas être divulgué à des personnes non autorisées comme l'indiquent des dispositions de la Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels.*

« Renseignement personnel ou nominatif » : *Renseignement qui concerne une personne physique et qui permet de l'identifier.*

« Réseau » : *Ensemble d'équipements qui sont reliés les uns aux autres par des câbles ou des faisceaux hertziens, afin qu'ils puissent échanger, distribuer ou diffuser des informations et partager différentes ressources.*

« 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.*

« Sécurité de l'information » : *Assurance, par un ensemble de mesures de sécurité, de rencontrer les objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.*

« Sinistre » : *Événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des dommages graves aux technologies de l'information du Ministère de sorte qu'elles ne sont plus opérantes et totalement inutilisables.*

« Standard » : *Norme qui n'a pas été définie ni entérinée par un organisme officiel de normalisation comme l'ISO, le CCN[13], 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.*

« Surveillance » : *Fonction permettant de détecter les vulnérabilités et les intrusions affectant les réseaux, les serveurs, les applications et les informations.*

[13] CCN : Conseil canadien des normes

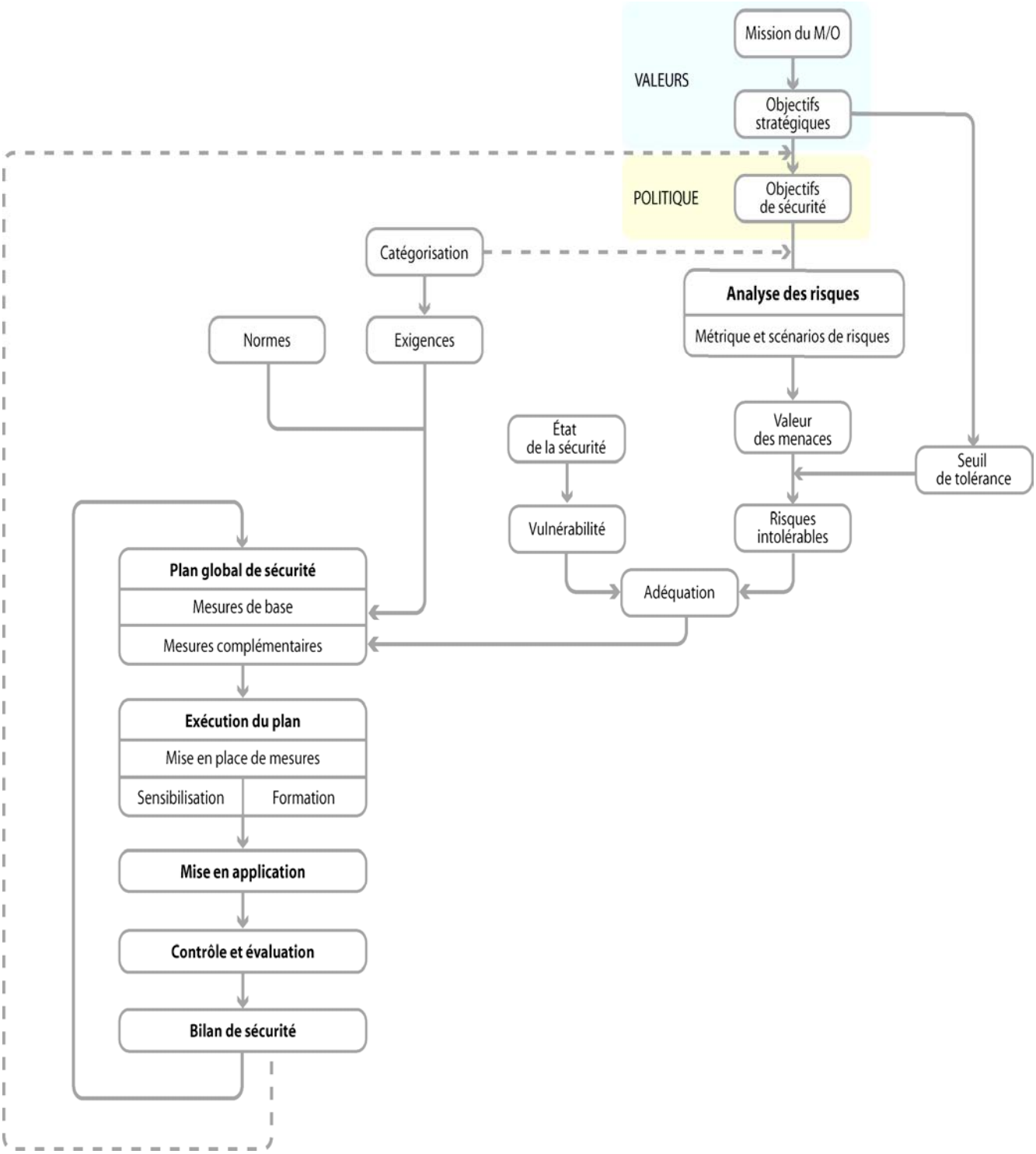
« Système d'information » : *Système constitué de l'équipement, des procédures, des ressources humaines, ainsi que des données qui y sont traitées, et dont le but est de fournir de l'information.*

« Technologie de l'information » *: Tout logiciel, matériel électronique ou combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, reproduire, protéger ou éliminer de l'information numérique.*

« Utilisateur » : *Toute personne du ministère ou organisme de quelque catégorie d'emploi, de statut d'employé ayant accès à l'actif informationnel, ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, accède à l'actif informationnel du ministère ou organisme.*

« Virus » *: Programme informatique infectieux, inséré dans un système informatique (ordinateur) dans le but d'exercer une action nuisible à son environnement.*

Annexe 2: Schéma du modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise



Annexe 3 : Dimensions de la sécurité (Extrait de l'AGSIN)

Dimension juridique	Aspects légaux	➢ Lois et règlements nationaux ➢ Lois et règlements provinciaux généraux et spécifiques ➢ Conventions internationales ➢ Contrats et ententes ➢ Avis juridiques
Dimension humaine	Sécurité appliquée au personnel	➢ Enquête de sécurité ➢ Habilitation sécuritaire ➢ Sensibilisation à la sécurité ➢ Formation du personnel
	Éthique, pratique professionnelle et imputabilité	➢ Responsabilités de l'organisation ➢ Responsabilités des gestionnaires ➢ Responsabilités du personnel et des usagers
Dimension organisationnelle	Sécurité administrative	➢ Politiques, normes, directives, guides et procédures de sécurité ➢ Rôles et responsabilités du personnel chargé de la sécurité ➢ Catégorisation de l'information ➢ Évaluation de vulnérabilité (menaces/risques) ➢ Registres et dossiers de sécurité ➢ Gestion du consentement ➢ Prévention
	Sécurité physique et du milieu	➢ Installations principales et auxiliaires des ressources informationnelles ➢ Contrôle de l'accès physique ➢ Sécurité du matériel
	Sécurité des opérations	➢ Administration ➢ Contrôle d'accès logique ➢ Surveillance et audit ➢ Utilisation et gestion des supports ➢ Mesure d'urgence, de relève et de continuité
Dimension technologique	Sécurité des logiciels, du matériel, des communications et des informations de sécurité	➢ Fonctions de sécurité : • Intégrité • Irrévocabilité • Identification/Authentification • Habilitation/Contrôle d'accès • Confidentialité • Disponibilité • Surveillance • Administration ➢ Développement des applications ➢ Sélection des applications ou équipements ➢ Installation et paramétrisation des applications ou équipements

Annexe 4 : Lois générales, directives, règlements, normes, guides et standards

Lois générales

- Code criminel (L.R. 1985, ch. C-46).
- Code civil du Québec (art. 35 à 41).
- Charte des droits et libertés de la personne (art. 5 et 44) : Garantit les libertés et droits fondamentaux de la personne afin que ceux-ci soient garantis par la volonté collective et mieux protégée contre toute violation.
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1) : s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par un organisme public ou par un tiers. Elle s'applique quelle que soit la forme de ces documents: écrite, graphique, sonore, visuelle, informatisée ou autre.
- Loi sur la sécurité civile : a pour objet la protection des personnes et des biens contre les sinistres. À cette fin, il encadre l'organisation de la sécurité civile dans ses principales dimensions que sont la prévention, la préparation des interventions, les interventions lors de tels évènements, réels ou imminents, et le rétablissement de la situation.
- Loi sur l'administration publique (L .R.Q.,c.A-6.01), un nouveau cadre de gestion pour la fonction publique, adopté le 25 mai 2000 : affirme la priorité accordée par l'Administration gouvernementale, dans l'élaboration et l'application des règles d'administration publique, à la qualité des services aux citoyens; elle instaure ainsi un cadre de gestion axé sur les résultats et sur le respect du principe de la transparence.
- Loi sur la fonction publique (L.R.Q., c. F-3.1.1), en particulier les dispositions du règlement traitant des normes d'éthique et de discipline dans la fonction publique québécoise.
- Loi sur les archives (L.R.Q., c. A-21.1), en ce qui a trait aux exigences relatives à la protection et la conservation des documents électroniques ayant une valeur patrimoniale ou archivistique.
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q.c.C-1.1),Gouvernement du Québec : a pour objet d'assurer notamment la sécurité juridique des communications effectuées au moyen de documents, l'équivalence fonctionnelle des documents et leur valeur juridique, quels qu'en soient les supports, ainsi que l'interchangeabilité de ces derniers. Elle vise également à assurer la concertation en vue d'harmoniser les systèmes, les normes et les standards techniques permettant la communication au moyen de documents technologiques.
- Loi modifiant diverses dispositions législatives eu égard à la divulgation de renseignements confidentiels en vue d'assurer la protection des personnes (L.Q.2001, chap.78).
- Loi sur le droit d'auteur (L.R.1985.ch. C42).

Directives et règlements

- ***La Directive sur la sécurité de l'information numérique et des échanges électroniques (CT 194055)*** est entrée en vigueur le 4 février 2000. Elle énonce les principes directeurs en matière de sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale, identifie les intervenants concernés par la gestion de cette sécurité, détermine les responsabilités des ministères et organismes et prévoit l'instauration des mécanismes de coordination et de collaboration appropriés en vue d'assurer la mise en œuvre d'un ensemble de mesures destinées à gérer les risques et leur impact à l'égard des objectifs du DICAI (disponibilité, intégrité, confidentialité de l'information numérique, authentification des utilisateurs et irrévocabilité des documents qu'ils rédigent ou des actions qu'ils posent).

- ***La Directive sur les services de certification offerts par le gouvernement du Québec (phase intérimaire)*** énonce les règles applicables aux services de certification de l'infrastructure à clés publiques gouvernementale (ICPG) et aux services de répertoire qui y sont afférents. Elle vise à assurer l'uniformité et la cohérence des exigences de certification au sein de l'Administration gouvernementale pendant la phase intérimaire du déploiement de l'ICPG.

- ***La Directive sur le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou un support informatique amovible (CT 193953), Conseil du trésor, octobre 1999.***

- ***La Directive sur l'utilisation éthique du courriel, d'un collecticiel, et des services d'Internet par le personnel de la fonction publique (C.T 198872 du 1er octobre 2002)*** précise les attentes minimales auxquelles tout membre du personnel de la fonction publique doit répondre lors de l'utilisation d'un accès gouvernemental au courriel, à un collecticiel et aux services d'Internet, au moyen de l'équipement électronique gouvernemental mis à sa disposition ou au moyen de l'équipement électronique de l'employé.

Normes, guides et standards

- ***La norme ISO/IEC 17799*** est issue de la norme britannique BS7799-1. Elle fournit un ensemble complet de mesures de contrôle comprenant une série de « bonnes pratiques » en matière de sécurité. Les bonnes pratiques (*« Business Best Practices »*) visent à réagir rapidement sans devoir réinventer la roue. BS7799 a deux parties mais seule BS7799-1 a acquis le statut de norme ISO, en décembre 2000. BS7799-1 explique le «quoi» et BS7799-2 explique le « comment ».

- ***Le Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise*** présente une démarche pour gérer la sécurité intégrant des mesures de base (normes et exigences de sécurité) et des mesures complémentaires (déterminées par une analyse des risques). Le schéma de ce modèle est joint en annexe 2.

- ***L'Architecture d'entreprise gouvernementale (AEG)*** est un exercice à haut niveau qui, en fonction des grands objectifs gouvernementaux, vise à améliorer la qualité des services et la performance de l'état, à comprendre, définir et illustrer la nouvelle prestation de services ainsi qu'à préciser la façon dont les ressources informationnelles (RI) pourront y contribuer. Plus spécifiquement, cette architecture se veut un modèle de référence (un outil) qui est mis à la disposition des ministères et organismes, leur permettant de positionner leurs projets et d'anticiper les opportunités de partage, de mise en commun et de réutilisation.

- ***L'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN)*** est un segment de l'Architecture d'entreprise gouvernementale (AEG) qui a pour objectif d'identifier et d'analyser les éléments architecturaux de haut niveau permettant au Secrétariat du Conseil du trésor (SCT) de promouvoir auprès des ministères et organismes une vision commune de la sécurité de l'information numérique. Il lui permet également de positionner sa démarche de mise en œuvre de composantes communes, partagées ou réutilisables de sécurité.

Des guides, élaborés par le Secrétariat du Conseil du trésor, sont également disponibles :

- ***Le guide relatif à la catégorisation des documents technologiques en matière de sécurité*** a pour objectif de fournir aux M/O un modèle de catégorisation permettant de créer une uniformité partout dans l'Administration publique afin que, à la suite de l'évaluation des risques et de la détermination des mécanismes de sécurité, le niveau de protection appliqué aux documents technologiques qui sont échangés entre les M/O et avec les utilisateurs soit adéquat.

- ***Le guide pour l'élaboration d'un plan de continuité des services*** se veut un cadre de référence pour appuyer les ministères et organismes dans l'élaboration d'un plan de continuité des services. Ce cadre de référence propose des outils pour faciliter l'élaboration des stratégies de reprise des services essentiels. Il permettra aux ministères et organismes d'élaborer et de mettre en place les mécanismes permettant de pallier à un désastre ou à tout événement qui pourrait engendrer une interruption des services essentiels sur une période jugée critique par l'organisation. Ce guide est conçu de façon à pouvoir combler les besoins tant au niveau des petites que des moyennes et grandes organisations gouvernementales.

- ***Le document « Pratique de vérification de la sécurité de l'information numérique »*** a pour objectif de soutenir les ministères et organismes dans la réalisation des objectifs suivants :

  - Mise en œuvre de la fonction « Contrôle et évaluation » ;
  - Appui à la reddition des comptes à l'occasion de la présentation du bilan annuel de sécurité ;
  - Appui aux intervenants en sécurité de l'information numérique pour la réalisation de vérifications limitées et peu complexes, l'expression des besoins et le suivi des mandats de vérification.

- ***Le guide de préparation du bilan de sécurité*** a pour objectif de guider les ministères et organismes dans l'utilisation de l'outil (questionnaire) ainsi que dans l'interprétation des résultats, tant pour les M/O en général que pour les infrastructures qu'ils fournissent. Ce document est divisé en deux parties : la première partie est un guide pour l'outil destiné à évaluer l'état général de la sécurité au

sein de chaque M/O. La deuxième partie est un guide pour l'outil réservé à l'évaluation de l'état de situation de ou des infrastructure(s) commune(s) fourni par les ministères et organismes.

- ***Le guide d'élaboration d'un programme de sensibilisation*** intègre deux fonctions principales. Dans un premier temps, il se veut un outil servant à élaborer un programme de sensibilisation avec tout ce qu'une telle démarche doit comporter (publics cibles, messages, calendrier, moyens techniques, etc.). C'est aussi, un outil d'accompagnement pour planifier et organiser une séance de sensibilisation (démarche pour organiser efficacement la séance, trucs pour rendre la communication plus efficace, etc.).

- ***Le document « Modèle et domaines de confiance de la sécurité et guide de conception »*** développe le concept et précise l'application au gouvernement d'un domaine de confiance de l'AGSIN. Ce domaine de confiance se définit comme un ensemble d'éléments d'ordre juridique, humain, organisationnel et technologique, un cadre de gestion de la sécurité et un ensemble d'activités pertinentes à la sécurité qui sont tous assujettis à une politique de sécurité administrée par une seule autorité en matière de sécurité.

- ***Le document « Contenu type et guide à l'élaboration d'une interface sécuritaire »*** élabore le contenu type d'une interface sécuritaire de l'AGSIN qui définit les modalités techniques de sécurisation de l'information numérique. L'interface sécuritaire est un ensemble d'éléments, comprenant à la fois des aspects logiciels et matériels, qui présente les normes et standards ainsi que les fonctions et mécanismes de sécurité nécessaires pour assurer la connectivité et l'interopérabilité entre les domaines de confiance ainsi qu'avec les clientèles.

- ***Le document « Contenu type et guide à l'élaboration d'une entente de sécurité »*** élabore le contenu type d'une entente de sécurité qu'un responsable d'un domaine de confiance devra élaborer et convenir pour ses échanges avec un autre domaine de confiance. Selon l'AGSIN, une entente de sécurité définit les règles qui régissent les interactions entre les domaines de confiance ainsi qu'avec les clientèles. Elle permet également de délimiter les champs de compétence entre les domaines de confiance. Une entente contient au minimum une interface sécuritaire.

Annexe 5 : Modèle de contenu type d'une ou (des) directive(s) de sécurité des actifs informationnels (modèle basé sur les éléments de la norme ISO/IEC 17799)

1. Portée

Ce document fournit des recommandations sur la gestion de la sécurité de l'information en vue de leur utilisation par les responsables de l'introduction, de la mise en œuvre ou du maintien de la sécurité au sein de leur organisation. Elle a pour objet de fournir une base commune pour l'élaboration des normes de sécurité des organisations et une méthode de gestion efficace de la sécurité en vue d'établir des rapports de confiance dans les transactions entre les organisations.

2. Terminologies et définitions

Voir lexique en annexe 1.

3. Politique globale de sécurité

3.1 Politique globale de sécurité de l'information

Objectif : Apporter une orientation et un soutien de la part de la direction à la sécurité de l'information.

Énoncé : Il convient que la direction définisse clairement l'orientation de la politique et démontre son soutien et son engagement en ce qui concerne la sécurité de l'information en diffusant et en mettant en œuvre sa politique globale de sécurité de l'information dans toute l'organisation.

- Document de politique globale de sécurité de l'information (voir modèle de contenu type d'une politique globale de sécurité à la section 7.5);
- Examen et évaluation.

4. Organisation de la sécurité

4.1 Infrastructure de la sécurité de l'information

Objectif : Gérer la sécurité de l'information au sein de l'organisation.

Énoncé : Il convient d'établir un cadre de gestion pour effectuer et contrôler la mise en œuvre de la gestion de la sécurité de l'information au sein de l'organisation Il convient d'établir des groupes de gestion appropriés, chargés de l'approbation de la politique de sécurité de l'information, de l'attribution des rôles de sécurité et de la coordination de la mise en œuvre de la sécurité dans toute l'organisation. Si nécessaire, il convient d'établir une source spécialisée de conseil concernant la sécurité de l'information et de la rendre accessible dans toute l'organisation. Il convient d'établir des contacts avec des spécialistes en sécurité externes à l'organisation, de façon à se tenir au courant des tendances industrielles, à contrôler les normes et les méthodes d'évaluation et à mettre en place des points de liaison appropriés pour faire face aux incidents de sécurité. Il convient d'encourager une démarche pluridisciplinaire en matière de sécurité de l'information, par exemple en faisant coopérer et collaborer les directeurs, les utilisateurs, les gestionnaires, les concepteurs d'applications, les vérificateurs et le personnel de sécurité ainsi que des spécialistes dans des domaines tels que l'assurance et la gestion des risques :

- Comité de sécurité de l'information
- Coordination de la sécurité de l'information
- Attribution des responsabilités de sécurité de l'information
- Processus d'autorisation pour les infrastructures de traitement de l'information
- Conseil de spécialistes de la sécurité de l'information
- Coopération entre les organismes
- Examen indépendant de sécurité de l'information

4.2 Sécurité des accès par des tiers

Objectif : Maintenir la sécurité des infrastructures de traitement de l'information de l'organisation et des actifs informationnels auxquels des tiers ont accès.

Énoncé : Il convient de contrôler les accès par des tiers aux infrastructures de traitement de l'information de l'organisation. En cas de nécessité professionnelle d'un tel accès par un tiers, il convient de procéder à une évaluation des risques afin de déterminer les implications au niveau de la sécurité et les exigences des mesures. Il convient également de valider les mesures à appliquer et de les définir sous forme de contrat avec le tiers en question. Il est possible que ces accès par des tiers impliquent également d'autres participants. Il convient d'inclure, dans les contrats accordant l'accès à un tiers, une clause pour la désignation d'autres participants éligibles ainsi que les conditions de leur accès. On pourrait utiliser la présente norme comme base pour de tels contrats de même que lorsque l'on envisage la sous-traitance du traitement de l'information.

- Identification des risques provenant de l'accès par des tiers
- Exigences de sécurité dans les contrats de tiers

4.3 Sous-traitance

Objectif : Maintenir la sécurité de l'information lorsque la responsabilité du traitement de l'information a été confiée à une autre organisation extérieure.

Énoncé : Il convient que les dispositions de sous-traitance abordent les risques, les mesures et les procédures de sécurité pour les systèmes d'information, les réseaux et/ou les environnements de bureau dans le contrat établi entre les parties.

- Exigences de sécurité dans les contrats de sous-traitance

5. Classification et contrôle des actifs

5.1 Responsabilités liées aux actifs

Objectif : Maintenir une protection appropriée des actifs de l'organisation.

Énoncé : Il convient que tout actif informationnel important fasse l'objet de responsabilités particulières et qu'ils aient un propriétaire désigné. La responsabilité concernant les actifs permet d'assurer le maintien d'un niveau adéquat de protection. Il convient d'identifier les détenteurs des actifs importants et d'attribuer les responsabilités du maintien de mesures appropriées. Les responsabilités de mise en oeuvre de ces mesures peuvent être déléguées, mais il convient que la responsabilité globale incombe aux détenteurs des actifs.

- Inventaire des actifs

5.2 Classification de l'information

Objectif : Faire en sorte que les actifs informationnels fassent l'objet d'un niveau de protection approprié.

Énoncé : Il convient que l'information soit classée afin d'indiquer les besoins, les priorités et le degré de protection. L'information présente divers degrés de sensibilité et d'importance. Certains éléments peuvent nécessiter un niveau de protection plus élevé ou un traitement spécial. Il convient d'utiliser un système de classification de l'information afin de définir un ensemble approprié de niveaux de protection et de communiquer la nécessité de mesures de traitement spéciales.

- Ligne directrices de classification
- Classification et traitement de l'information

6. Sécurité appliquée au personnel

6.1 Sécurité dans la définition des postes et des ressources

Objectif : Réduire les risques d'erreur humaine, de vol, de fraude ou d'utilisation abusive des infrastructures.

Énoncé : Il convient d'aborder les responsabilités en matière sécurité au stade du recrutement, de les inclure dans les descriptions de postes et de les surveiller au cours de la période d'emploi d'un individu. Il convient que tous les candidats soient sélectionnés de façon appropriée, en particulier pour les postes critiques. Il convient que tous les employés et les utilisateurs des structures de traitement de l'information extérieurs à l'organisation signent un accord de confidentialité (non divulgation).

- Inclusion de la sécurité dans les responsabilités des postes
- Sélection du personnel et politique de recrutement
- Accords de confidentialité
- Condition d'emploi

6.2 Formation des utilisateurs

Objectif : Faire en sorte que les utilisateurs soient sensibilisés aux menaces et aux préoccupations relatives à la sécurité de l'information et qu'ils soient en mesure de soutenir la politique de sécurité de l'organisation dans le cadre normal de leur travail.

Énoncé : Il convient que les utilisateurs soient formés sur les procédures de sécurité et sur l'utilisation correcte des infrastructures de traitement de l'information afin de minimiser les risques de sécurité possibles.

- Éducation et formation sur la sécurité de l'information

6.3 Réactions aux incidents de sécurité et aux défauts de fonctionnement

Objectif : Minimiser les dommages provenant d'incidents de sécurité et de défauts de fonctionnement, surveiller ces incidents et en tirer des leçons.

Énoncé : Il convient que les incidents affectant la sécurité soient signalés le plus rapidement possible par l'intermédiaire des filières de gestion appropriées. Il convient que tous les employés et tous les fournisseurs soient informés des procédures utilisées pour le signalement des différents types d'incidents (infraction à la sécurité, menace, faiblesse ou mauvais fonctionnement) qui pourraient avoir un impact sur la sécurité des actifs de l'organisation. Il convient d'exiger d'eux qu'ils signalent le plus rapidement possible au point de contact désigné tout incident observé ou soupçonné. Il convient que l'organisation établisse un processus disciplinaire officiel destiné aux employés coupables d'infractions

à la sécurité. De manière à pouvoir réagir correctement à ces incidents, il pourra s'avérer nécessaire de recueillir des éléments de preuve dès que possible après la survenance de ces incidents.

- Signalement des incidents de sécurité
- Signalement des failles de sécurité
- Signalement du fonctionnement défectueux de logiciels
- Leçons à tirer des incidents
- Processus disciplinaires

7. Sécurité physique et sécurité de l'environnement

7.1 Zones de sécurité

Objectif : Empêcher l'accès non autorisé aux locaux et aux informations du ministère ou organisme ainsi que les dommages et les perturbations de ces locaux et de ces informations.

Énoncé : Il convient que les infrastructures de traitement de l'information cruciales ou sensibles de l'organisation soient situées dans des zones de sécurité, protégées par un périmètre de sécurité défini, avec des barrières de sécurité et des mesures de contrôle appropriées à l'entrée. Il convient qu'elles soient protégées physiquement contre tout accès non autorisé, contre tout dommage et contre toute perturbation. Il convient que la protection corresponde aux risques identifiés. Il est recommandé d'adopter une politique de bureaux et d'écrans dégagés afin de réduire le risque d'accès non autorisés ou de dommages subis par des papiers, des supports informatiques et des infrastructures de traitement de l'information.

- Périmètre de sécurité physique
- Mesures physiques à l'entrée
- Sécurisation des bureaux, de salles et des infrastructures
- Travail dans les zones de sécurité
- Isolation de zones de livraison et de chargement

7.2 Sécurité du matériel

Objectif : Empêcher toute perte, dommage ou compromission des actifs et toute interruption des activités du ministère ou organisme.

Énoncé : Il convient que le matériel soit protégé physiquement contre les menaces d'atteinte à la sécurité et les dangers liés à l'environnement. Il est nécessaire de protéger le matériel informatique (y compris celui utilisé hors du site) afin de réduire les risques d'accès non autorisés aux données et d'assurer une protection contre les pertes et les dommages. Il convient également d'être attentif à l'emplacement et à la mise au rebut du matériel. Il est possible que des mesures spéciales soient requises afin d'assurer la protection contre des dangers ou des accès non autorisés et de protéger les infrastructures de soutien, telles que les infrastructures d'alimentation électrique et de câblage.

- Emplacement et protection du matériel

- Alimentation électrique
- Sécurité du câblage
- Maintenance du matériel
- Sécurité du matériel utilisé à l'extérieur des locaux
- Mise au rebut ou réutilisation du matériel en toute sécurité

7.3 Mesures générales

Objectif : Empêcher la compromission ou le vol de l'information et des infrastructures de traitement de l'information.

Énoncé : Il convient de protéger l'information et les infrastructures de traitement de l'information contre leur divulgation à des personnes non autorisées et contre leur modification ou leur vol par des personnes non autorisées et il faut que des mesures soient en place afin de minimiser les pertes ou les dommages.

- Politique de bureaux et d'écran dégagés
- Enlèvement des biens

8. Gestion des communications et des opérations

8.1 Procédures et responsabilités opérationnelles

Objectif : Assurer le fonctionnement correct et sûr des infrastructures de traitement de l'information.

Énoncé : Il convient d'établir les responsabilités et les procédures de gestion et d'utilisation de toutes les infrastructures de traitement de l'information. Cela comprend l'élaboration de consignes d'utilisation et de procédures de réaction aux incidents appropriées. S'il y a lieu, il convient de diviser les responsabilités afin de réduire le risque d'une utilisation abusive négligente ou délibérée du système.

- Procédures opérationnelles documentées
- Contrôle des modifications opérationnelles
- Procédures de gestion des incidents
- Division des responsabilités
- Séparation des infrastructures de développement et des infrastructures opérationnelles
- Gestion externe des infrastructures

8.2 Planification et acceptation des systèmes

Objectif : Minimiser les risques de défaillances des systèmes. Une planification et une préparation préalables sont nécessaires pour assurer la disponibilité de capacités et de ressources suffisantes.

Énoncé : Il convient de faire des prévisions sur les exigences de capacité future afin de réduire le risque de surcharger les systèmes. Il convient d'établir, de documenter et de soumettre à des essais les exigences opérationnelles des nouveaux systèmes avant de les accepter et de les utiliser.

- Planification de capacité
- Acceptation des systèmes

8.3 Protection contre les logiciels pernicieux

Objectif : Protéger l'intégrité des logiciels et de l'information.

Énoncé : Il est nécessaire de prendre des précautions afin d'empêcher et de détecter l'introduction de logiciels pernicieux. Les logiciels et les infrastructures de traitement de l'information sont vulnérables à l'introduction de logiciels pernicieux, comme les virus informatiques, les vers de réseau, les chevaux de Troie et les bombes logiques. Il convient de sensibiliser les utilisateurs aux dangers présentés par les logiciels non autorisés ou pernicieux et les responsables doivent, s'il y a lieu, introduire des mesures spéciales pour empêcher ou détecter leur introduction. En particulier, il est indispensable de prendre des précautions afin de détecter et d'empêcher la présence de virus informatiques sur les ordinateurs personnels.

- Mesures contre les logiciels pernicieux

8.4 Intendance

Objectif : Maintenir l'intégrité et la disponibilité des services de traitement de l'information et de communication.

Énoncé : Il convient d'établir des procédures de routine pour la mise en œuvre de la stratégie convenue concernant la sauvegarde en faisant des copies de sauvegarde des données et en s'exerçant à les récupérer au bon moment, en consignant les événements et les défauts et, le cas échéant, en surveillant l'environnement du matériel.

- Sauvegarde des informations
- Journaux des opérateurs
- Consignation des défauts

8.5 Gestion des réseaux

Objectif : Assurer la protection de l'information dans les réseaux et la protection des infrastructures de soutien.

Énoncé : La gestion de la sécurité de réseaux informatiques, qui peut dépasser les frontières organisationnelles, nécessite une attention particulière. Des mesures spéciales peuvent également être requises pour la protection de données sensibles empruntant des réseaux publics.

- Mesure de contrôle des réseaux

8.6 Manipulation et sécurité des supports

Objectif : Empêcher les dommages causés aux actifs et l'interruption des activités du ministère ou organisme.

Énoncé : Il convient que les supports informatiques soient contrôlés et protégés physiquement. Il convient d'établir des procédures opérationnelles appropriées pour la protection des documents, des supports informatiques (bandes, disques, cassettes), des données entrée/sortie et de la documentation des systèmes contre les dommages, le vol et les accès non autorisés.

- Gestion des supports informatiques amovibles
- Mise au rebut des supports
- Procédures de manipulation de l'information
- Sécurité des documentations de systèmes

8.7 Échanges d'informations et de logiciels

Objectif : Empêcher toute perte, modification ou utilisation abusive des informations échangées entre des organisations.

Énoncé : Il convient de contrôler les échanges d'information et de logiciels entre les organisations et ceux-ci doivent respecter toute législation applicable. Il convient que ces échanges soient basés sur des accords. Il convient d'établir des procédures et des normes de protection des informations et des supports en transit. Il convient de prendre en considération les implications pour l'organisation et celles relatives à la sécurité associées à l'échange de données électroniques, au commerce électronique et au courrier électronique et de considérer les mesures nécessaires.

- Accords sur les échanges d'informations et de logiciels
- Sécurité des supports en transit
- Sécurité du commerce électronique
- Sécurité du courrier électronique
- Sécurité des systèmes bureautiques
- Systèmes disponibles au public
- Autres formes d'échange d'information

9. Contrôle des accès logiques

9.1 Exigences du ministère ou organisme concernant le contrôle des accès logiques

Objectif : Contrôler l'accès aux informations.

Énoncé : Il convient de contrôler l'accès aux informations et aux procédés opérationnels en se basant sur les exigences de l'organisation et sur les exigences de sécurité. Il convient que ce contrôle tienne compte des politiques de dissémination de l'information et d'autorisation d'accès à l'information.

- Politique de contrôle des accès logiques

9.2 Gestion des accès utilisateurs

Objectif : Empêcher les accès non autorisés aux systèmes d'information.

Énoncé : Il convient que des procédures officielles soient en place pour contrôler l'attribution des droits d'accès aux systèmes et aux services d'information. Il convient que ces procédures couvrent tous les stades dans le cycle de vie des accès utilisateur, depuis l'enregistrement initial des nouveaux utilisateurs jusqu'à l'annulation finale de l'enregistrement des utilisateurs qui n'ont plus besoin d'avoir accès aux systèmes et aux services d'information. Il convient de prêter une attention particulière, le cas échéant, à la nécessité de contrôler l'attribution des droits d'accès privilégiés permettant aux utilisateurs d'outrepasser les mesures de contrôle du système.

- Enregistrement des utilisateurs
- Gestion des privilèges
- Gestion de mots de passe d'utilisateur
- Examen des droits d'accès utilisateur

9.3 Responsabilités des utilisateurs

Objectif : Empêcher l'accès par des utilisateurs non autorisés.

Énoncé : Pour une sécurité efficace, la coopération des utilisateurs autorisés est indispensable. Il convient d'informer les utilisateurs de leurs responsabilités en ce qui concerne le maintien de mesures de contrôle d'accès efficaces, en particulier en ce qui concerne l'utilisation des mots de passe et la sécurité du matériel utilisateur.

- Utilisation des mots de passe
- Matériel utilisateur sans surveillance

9.4 Contrôle de l'accès aux réseaux

Objectif : Protection des services sur réseau.

Énoncé : Il convient de contrôler l'accès aux services internes et externes sur réseau. Cela est nécessaire afin d'empêcher que les utilisateurs qui ont accès aux réseaux et aux services sur réseau compromettent la sécurité de ces services sur réseau en assurant :
a) la présence d'interfaces appropriées entre le réseau de l'organisation et les réseaux appartenant à d'autres organisations ou les réseaux publics;
b) la présence de mécanismes d'authentification appropriés pour les utilisateurs et le matériel à distance;
c) le contrôle de l'accès utilisateur aux services d'information.

- Politique sur l'utilisation des services sur réseaux
- Itinéraire obligatoire
- Authentification des utilisateurs pour les connexions externes
- Authentification des nœuds
- Protection des ports de diagnostic à distance
- Isolation au sein des réseaux
- Contrôle des connexions réseau
- Contrôle du routage des réseaux
- Sécurité des services de réseau

9.5 Contrôle de l'accès aux systèmes d'exploitation

Objectif : Empêcher tout accès non autorisé aux systèmes d'exploitation.

Énoncé : Il convient d'utiliser des dispositifs de sécurité au niveau du système d'exploitation afin de limiter l'accès aux ressources contrôlées ou exploitées par ce système. Ces dispositifs doivent remplir les fonctions suivantes :

a) l'identification et la vérification de l'identité, et si besoin est, du terminal ou du site de chacun des utilisateurs autorisés;
b) l'enregistrement des accès au système, qu'ils soient réussis ou non;
c) la prévision d'un moyen d'authentification approprié; si un système de gestion des mots de passe est utilisé, il convient qu'il assure la qualité des mots de passe;
d) le cas échéant, la restriction des heures de connexion des utilisateurs.

Il existe d'autres méthodes de contrôle d'accès, comme celle de l'interrogation réponse au cas où leur utilisation serait justifiée en raison des risques courus par le ministère ou organisme.

- Identification automatique du terminal
- Procédures de connexion de terminal
- Identification et authentification des utilisateurs
- Système de gestion des mots de passe

- Utilisation des programmes utilitaires
- Avertisseurs individuels pour la protection des utilisateurs
- Fonction d'arrêt à délai d'inactivité de terminal
- Limitation du temps de connexion

9.6 Contrôle de l'accès aux applications

Objectif : Empêcher tout accès non autorisé à l'information détenue sur des systèmes d'information.

Énoncé : Il convient d'utiliser des dispositifs de sécurité afin de restreindre l'accès au sein des systèmes d'applications. Il convient de restreindre aux utilisateurs autorisés l'accès logique aux logiciels et à l'information. Il convient que les systèmes d'applications doivent :

a) contrôler l'accès des utilisateurs à l'information et aux fonctions des systèmes d'applications conformément à une politique définie de contrôle des accès de l'organisation;

b) fournir une protection contre l'accès non autorisé à tout programme utilitaire et à tout logiciel de système d'exploitation capable d'outrepasser les commandes du système ou des applications;

c) ne pas porter atteinte à la sécurité des autres systèmes avec lesquels les ressources d'information sont partagées;

d) être capables de fournir l'accès aux informations uniquement au propriétaire, à d'autres individus autorisés ou à des groupes définis d'utilisateurs.

- Restriction des accès à l'information
- Isolation des systèmes critiques

9.7 Surveillance des accès aux systèmes et de leur utilisation

Objectif : Détecter les activités non autorisées.

Énoncé : Il convient de surveiller les systèmes afin de détecter tout écart de la politique de contrôle des accès et d'enregistrer les événements pouvant être surveillés afin d'avoir des éléments de preuve en cas d'incidents de sécurité. La surveillance des systèmes permet de vérifier l'efficacité des mesures adoptées ainsi que leur conformité à un modèle de politique d'accès.

- Consignation des événements
- Surveillance de l'utilisation des systèmes
- Synchronisation des horloges

9.8 Informatique mobile et télétravail

Objectif : Assurer la sécurité de l'information lorsqu'on utilise des unités informatiques mobiles ou des installations de télétravail.

Énoncé : Il convient que la protection fournie corresponde aux risques présentés par ces méthodes spécifiques de travail. Lorsqu'on utilise l'informatique mobile, il convient d'examiner les risques présentés par le fait qu'on travaille dans un environnement non protégé et de mettre en place une protection appropriée. Dans le cas du télétravail, il convient que l'organisation applique une protection sur le site de télétravail et veille à ce que des dispositions appropriées soient prises pour ce type de travail.

- Informatique mobile
- Télétravail

10. Développement et maintenance des systèmes

10.1 Exigences de sécurité des systèmes

Objectif : Faire en sorte que la sécurité soit incorporée aux systèmes d'information. Cela comprend les infrastructures, les applications de l'organisation et les applications développées par les utilisateurs. La conception et la mise en œuvre du processus professionnel soutenant l'application ou le service peuvent être cruciales pour la sécurité.

Énoncé : Il convient d'identifier les exigences de sécurité et de valider celles-ci avant le développement de systèmes d'information. Il convient que toutes les exigences de sécurité, y compris la nécessité de dispositions de substitution, soient identifiées au stade des exigences du projet et justifiées, approuvées et documentées comme faisant partie des arguments généraux de l'organisation en faveur d'un système d'information.

- Analyse et spécification des exigences de sécurité

10.2 Sécurité des systèmes d'applications

Objectif : Empêcher les pertes, les modifications ou les utilisations abusives des données utilisateur dans les systèmes d'applications.

Énoncé : Il convient d'incorporer dans les systèmes d'applications, y compris dans les applications écrites par les utilisateurs, des mesures appropriées et des traces d'audit ou des journaux d'activités. Ces mesures doivent comprendre la validation des données d'entrée, du traitement interne et des données de sortie. Il est possible que des mesures supplémentaires soient nécessaires pour les systèmes qui traitent des actifs critiques, précieux ou cruciaux de l'organisation ou qui ont un impact sur ceux-ci.

Il convient de déterminer ces mesures en se basant sur les exigences de sécurité et sur l'évaluation des risques

- Validation des données d'entrée
- Contrôle du traitement interne
- Authentification des messages
- Validation des données de sortie

10.3 Mesures cryptographiques

Objectif : Protéger la confidentialité, l'authenticité ou l'intégrité de l'information.

Énoncé : Il convient d'utiliser des systèmes et des techniques cryptographiques pour protéger l'information considérée comme étant exposée à des risques et pour laquelle d'autres mesures ne fournissent pas de protection adéquate.

- Politique sur l'utilisation des mesures cryptographiques
- Cryptage
- Signatures numériques
- Services de non-répudiation
- Gestion des clés

10.4 Sécurité des fichiers

Objectif : Faire en sorte que les projets informatiques et les activités de soutien soient exécutés d'une façon sécurisée.

Énoncé : Il convient de contrôler les accès aux fichiers système. Il convient que le maintien de l'intégrité des applications incombe aux groupements utilisateurs ou au groupe de développement auquel appartient l'application ou le logiciel.

- Contrôle des logiciels opérationnels
- Protection des données d'essai des systèmes
- Contrôle de l'accès aux bibliothèques de programmes sources

10.5 Sécurité des environnements de développement et de soutien

Objectif: Maintenir la sécurité des logiciels et des informations des systèmes d'applications.

Énoncé : Il convient de contrôler rigoureusement les environnements de projets et de soutien. Il convient que les responsables des applications soient également responsables de la sécurité des environnements de projets ou de soutien. Il convient qu'ils fassent en sorte que toutes les modifications proposées du système soient examinées pour s'assurer que ces modifications ne portent pas atteinte à la sécurité du système ni à celle de l'environnement opérationnel.

- Procédures de contrôle des modifications
- Examen technique des modifications apportées au système d'exploitation

- Restrictions sur les modifications apportées aux progiciels
- Voies secrètes et codes Troie
- Développement sous-traité des logiciels

11. Gestion de la continuité des activités

11.1 Aspects de la gestion de la continuité des activités de l'organisation

Objectif : Parer aux interruptions des activités de l'organisation et protéger les processus cruciaux de l'organisation contre les effets des défaillances majeures ou des sinistres informatiques.

Énoncé : Il convient qu'un processus de gestion de la continuité des activités de l'organisation soit mis en œuvre afin de réduire toute perturbation causée par des sinistres informatiques et des défaillances de sécurité (qui pourraient résulter par exemple de catastrophes naturelles, d'accidents, de défaillances de matériel et d'actions intentionnelles) à un niveau acceptable au moyen d'une combinaison de mesures préventives et de rétablissement. Il convient d'analyser les conséquences des sinistres informatiques, des défaillances de sécurité et des pertes de service. Il convient d'élaborer et de mettre en œuvre des plans d'urgence afin de permettre de rétablir les processus de l'organisation dans les délais requis. Il convient de maintenir ces plans et de les mettre en pratique afin qu'ils fassent partie intégrante de tous les autres processus de gestion. La gestion de la continuité des activités de l'organisation doit comprendre des mesures permettant d'identifier et de réduire les risques, de limiter les conséquences des incidents préjudiciables et de permettre le rétablissement en temps opportun des opérations essentielles.

- Processus de gestion de la continuité des activités de l'organisation
- Continuité des activités de l'organisation et analyse des répercussions
- Création et mise en œuvre des plans de continuité
- Cadre de planification de la continuité des activités de l'organisation

12. Conformité

12.1 Conformité aux exigences légales

Objectif: Éviter les infractions à toute obligation d'ordre pénal et civil, légal, réglementaire ou contractuel et à toute exigence de sécurité. Il est possible que la conception, le fonctionnement, l'utilisation et la gestion des systèmes d'information fassent l'objet d'exigences de sécurité légales, réglementaires et contractuelles.

Énoncé : Il convient de consulter les conseillers juridiques de l'organisation ou des hommes de loi adéquatement qualifiés en ce qui concerne les exigences légales spécifiques. Celles-ci varient d'un pays à un autre et elles peuvent être différentes pour les informations créées dans un pays et transmises dans un autre pays (c'est-à-dire pour les flux transfrontières de données).

- Identification de la législation applicable
- Droits de propriété intellectuelle (DPI)
- Protection de la pérennité des informations de l'organisation

- Protection des données et confidentialité des renseignements personnels
- Prévention de toute utilisation abusive des infrastructures de traitement de l'information
- Réglementation des mesures cryptographiques
- Collecte d'éléments de preuve

12.2 Examens de la politique de sécurité et de la conformité technique

Objectif : Assurer la conformité des systèmes aux politiques et aux normes de sécurité de l'organisation.

Énoncé : Il convient d'effectuer, à intervalles réguliers, des examens de la sécurité des systèmes d'information. Il convient que ces examens s'effectuent au regard des politiques de sécurité appropriées et que les plates-formes techniques ou les systèmes d'information soient vérifiés quant à leur conformité aux normes de mise en œuvre de la sécurité.

- Conformité à la politique de sécurité
- Contrôle de conformité technique

12.3 Considérations sur les audits des systèmes

Objectif : Maximiser l'efficacité du processus d'audit des systèmes et minimiser toute perturbation causée et subie par le processus d'audit.

Énoncé : Il convient qu'il existe des mesures pour protéger les systèmes opérationnels et les instruments d'audit au cours des audits de systèmes Une protection est également requise afin de protéger l'intégrité et d'empêcher les utilisations abusives des instruments d'audits.

- Mesures de contrôle d'audit des systèmes
- Protection des outils d'audit des systèmes