Ministère de l'Emploi et de la Solidarité sociale
Québec

POLITIQUE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

5 mars 2009

TABLE DES MATIÈRES

1 Introduction

Pour accomplir ses mandats, le ministère de l'Emploi et de la Solidarité sociale (MESS) recueille, conserve, traite, diffuse et archive d'importantes quantités d'informations dont la masse va toujours augmenter au fil des années. Ces informations sont nécessaires à la réalisation de sa mission et requièrent une protection tout au long de leur cycle de vie. Avec l'évolution des technologies de l'information, l'information numérique a pour sa part pris une place prépondérante dans les activités courantes du Ministère.

Conscient du rôle stratégique de ses informations, le Ministère s'est doté, en mai 2000, d'une politique relative au domaine de la gestion de la sécurité de l'information numérique et de ses échanges électroniques. En vigueur depuis huit ans, cette politique se devait d'être revue, notamment afin de tenir compte des exigences découlant de la nouvelle Directive[1] sur la sécurité de l'information gouvernementale (C.T. 203560) qui est entrée en vigueur au mois de mai 2006. Cette dernière remplace l'ancienne Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale (C.T. 194055). Elle élargit le spectre de la gestion de la sécurité. En outre, elle assigne au sous-ministre ou au dirigeant de tout organisme public l'ultime responsabilité de la sécurité de l'information sous son autorité. La présente politique fait donc partie des actions que le MESS prend pour mettre en application cette Directive gouvernementale (C.T. 203560).

D'autre part, le contexte organisationnel d'ensemble du Ministère s'est considérablement transformé au cours des dernières années. L'utilisation de plus en plus répandue des nouvelles technologies de l'information (NTIC) et l'usage accentué de l'Internet en particulier ont également eu d'importants impacts sur l'organisation du travail.

Outre ces deux grandes tendances d'ensemble qui ont affecté le fonctionnement du Ministère, le gouvernement du Québec, pour sa part, fait de la mise en place du gouvernement en ligne l'une de ses priorités en vue d'assurer aux citoyens du Québec des services publics plus accessibles. Le MESS, déjà fortement engagé dans cette orientation, est appelé à accroître sa prestation de services en ligne, accentuant de ce fait l'importance de la sécurité de l'information.

Le 22 novembre 2007, le gouvernement du Québec annonçait le regroupement des ressources et des infrastructures en technologies de l'information du Ministère à celles du *Centre de services partagés du Québec (CSPQ)*. Des chantiers de travail ont aussitôt été constitués et leurs travaux ont porté sur la mise en œuvre de l'Entente de transfert des ressources et des infrastructures technologiques du ministère de l'Emploi et de la Solidarité sociale au Centre de services partagés du Québec dès le 1er avril 2008, et ce, dans un contexte d'impartition des services en technologies de l'information rendus au Ministère.

[1] Directive gouvernementale sur la sécurité de l'information gouvernementale, ministère des Services gouvernementaux, CT 203560 du 11 avril 2006.

2 Contexte

2.1 Cadre juridique

La gestion de la sécurité de l'information s'effectue dans le respect des lois et règlements auxquels le Ministère est soumis. Ceux-ci ont une portée générale ou encore sectorielle. Les lois à portée générale sont :

- Loi sur l'administration publique (L.R.Q., c. A-6.01) ;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1) ;
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1) ;
- Loi sur les archives (L.R.Q., c. A-21.1) ;
- Loi sur la sécurité dans les édifices publics (L.R.Q., c. S-3) ;
- Loi fédérale sur les droits d'auteur (L.R. 1985, c. C-42);
- Charte des droits et libertés de la personne (L.R.Q., c. C-12, art. 5 et 44) ;
- Code civil du Québec, (art. 37 à 41);
- Directive sur la sécurité de l'information gouvernementale (C.T. 203560);
- 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);
- Règlement sur l'éthique et la discipline dans la fonction publique (LRQ, chap. F-3.1.1, art. 126, paragraphes 1 à 3);
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (décret 408-2008, art.7).

La gestion de la sécurité de l'information est également soumise à certaines exigences découlant de lois et règlements propres à l'environnement d'affaires du Ministère. Ces lois et règlements auront également à être pris en compte lors de l'établissement des mesures de la sécurité de l'information[2].

2.2 Cadre normatif

2.2.1 Cadre normatif gouvernemental

La Directive sur la sécurité de l'information gouvernementale (C.T. 203560) est le document de référence en matière de gestion de la sécurité de l'information. Cette directive identifie les principaux rôles en ce domaine et attribue à ceux-ci des responsabilités précises. La présente politique vise ainsi à établir le cadre de gestion applicable à la sécurité de l'information du Ministère, en s'appuyant en outre sur les obligations énoncées par cette directive gouvernementale.

[2] La liste des lois et règlements spécifiques est disponible dans l'Intranet corporatif.

2.2.2 Cadre normatif ministériel

Le Ministère a déjà adopté un certain nombre de politiques qui visent à assurer la sécurité de l'information. Ces politiques ministérielles sont les suivantes :

- Politique concernant le « domaine de la gestion de la sécurité de l'information numérique et des échanges électroniques » ;
- Politique ministérielle en matière de vérification interne ;
- Politique ministérielle sur la sécurité physique dans les édifices du MESS ;
- Politique ministérielle sur la gestion documentaire ;
- Politique éditoriale et cadre de gestion de l'intranet ministériel du MESS;
- Politique éditoriale des sites Internet du MESS.

Pour répondre à ses besoins spécifiques en la matière, le Ministère s'est également doté des documents normatifs suivants :

- Lignes directrices sur l'utilisation et la gestion du réseau Internet et du courrier électronique ;
- Guides et bulletins d'information sur les bonnes pratiques en matière de protection des renseignements personnels;
- Guide sur L'Éthique au MESS – Agir avec intégrité ;
- Guide relatif à la gestion des droits d'accès aux ressources informatiques par les unités administratives du Ministère ;
- Plusieurs pratiques et procédures relatives à la sécurité informatique (référence: le coffre à outils des Technologies de l'information);
- Cadre de gestion sur l'utilisation de la vidéosurveillance ;
- Cadre ministériel de gestion des sondages auprès des personnes ;
- Registre d'autorité de la sécurité de l'information numérique;
- Procédures de traitement du matériel informatique en surplus ;
- Procédures relatives à la destruction sécuritaire des documents sur support papier ;
- Protocole d'identification à appliquer lors de communications avec les clientèles;
- Procédures de gestion de la sécurité physique et des accès;
- Directive ministérielle sur la réclamation lors de pertes matérielles subies par le Ministère;

Il y a quelques années, le Ministère a aussi élaboré une stratégie de communication visant à rappeler à l'ensemble de son personnel l'importance d'adopter un comportement responsable au regard de l'éthique, de la protection des renseignements personnels, de l'application des lignes directrices sur l'utilisation du réseau Internet et du courrier électronique de même qu'en matière de sécurité de l'information numérique.

3 Objectifs, principes directeurs et orientations ministérielles

3.1 Objectifs

L'objectif premier de cette politique consiste à réaffirmer l'engagement du Ministère à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information et à établir les grands principes et orientations qui guideront son action en cette matière.

De plus, elle a pour objectifs spécifiques de :

- Définir une structure de gestion de la sécurité de l'information ;
- Définir les mécanismes de coordination et de concertation entre les différents intervenants de la sécurité de l'information ;
- Déterminer les rôles clés et identifier les principales responsabilités aux fins de la gestion de la sécurité de l'information, et ce, à tous les niveaux de l'organisation.

Cette politique constitue l'élément de base pour la mise en place du processus de gestion intégrée de la sécurité de l'information au Ministère.

3.2 Principes directeurs gouvernementaux

La présente politique s'appuie, en premier lieu, sur les objectifs énoncés par la Directive sur la sécurité de l'information gouvernementale (C.T. 203560) et qui sont les suivants :

- La sécurité de l'information gouvernementale doit permettre de maintenir et de rehausser la confiance à l'égard de l'État et des services publics qu'il rend;
- Les mesures de sécurité doivent être proportionnelles à la valeur de l'information gouvernementale à protéger et être établies en fonction des risques encourus et de leurs impacts.

De plus, elle se conforme aux principes directeurs suivants qui ont été également énoncés dans cette Directive gouvernementale:

Responsabilité et imputabilité

L'efficacité de la sécurité de l'information exige l'attribution claire de responsabilités à tous les niveaux de l'organisation et la mise en place d'un processus de gestion interne de la sécurité permettant une reddition de comptes adéquate.

Évolution

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

Universalité

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

Éthique

Le processus de gestion de la sécurité de l'information doit être soutenu par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

3.3 Orientations ministérielles en matière de sécurité de l'information

La capacité du Ministère à assurer la sécurité de l'information qu'il détient et qu'il utilise dans l'exercice de ses responsabilités est l'une des conditions essentielles à l'établissement d'un lien de confiance solide avec les citoyens et avec l'ensemble de ses partenaires. Ceux-ci lui confient en outre des renseignements personnels et ils comptent sur lui pour en assurer la confidentialité et pour obtenir des services qui sont fiables et rendus en temps opportun.

La gestion sécuritaire de l'information constitue donc un défi important que le Ministère doit relever dans l'accomplissement de sa mission. À cette fin, il doit se doter des mesures de sécurité appropriées qui lui permettront de gérer adéquatement les risques qu'il pourrait encourir en matière de sécurité de l'information.

4 Portée

La présente politique s'applique à l'information gouvernementale, qui est consignée dans un document au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1) et qui peut être communiquée par tout moyen. L'information visée est celle que le Ministère détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

L'ensemble des employés du Ministère est régi par cette politique, et ce, à tous les niveaux d'interventions : stratégique, tactique et opérationnel.

Elle s'applique également aux fournisseurs et aux partenaires du Ministère qui peuvent avoir accès à cette information. À cet égard, les ententes qui lient le Ministère avec ces organismes contiendront les clauses types appropriées pour satisfaire aux exigences de sécurité de l'information établies par le Ministère.

5 Structure

La structure fonctionnelle est divisée selon trois niveaux d'intervention : stratégique, tactique et opérationnel.

5.1 Les niveaux d'intervention

Au **niveau stratégique** de la gestion de sécurité de l'information du Ministère, nous retrouvons en premier lieu le sous-ministre qui est le premier responsable de la sécurité de l'information relevant de son autorité. À cet égard, il préside le Comité ministériel de la protection des renseignements personnels et de la sécurité de l'information (CMPRPSI). Il approuve également le cadre normatif applicable à la sécurité de l'information du Ministère, désigne les principaux intervenants dont le responsable de la sécurité de l'information (RSI[3]) et, en lien avec les valeurs organisationnelles, il définit les orientations en la matière. Pour sa part, le RSI représente et assiste le sous-ministre en matière de gestion et de coordination de la sécurité de l'information au Ministère.

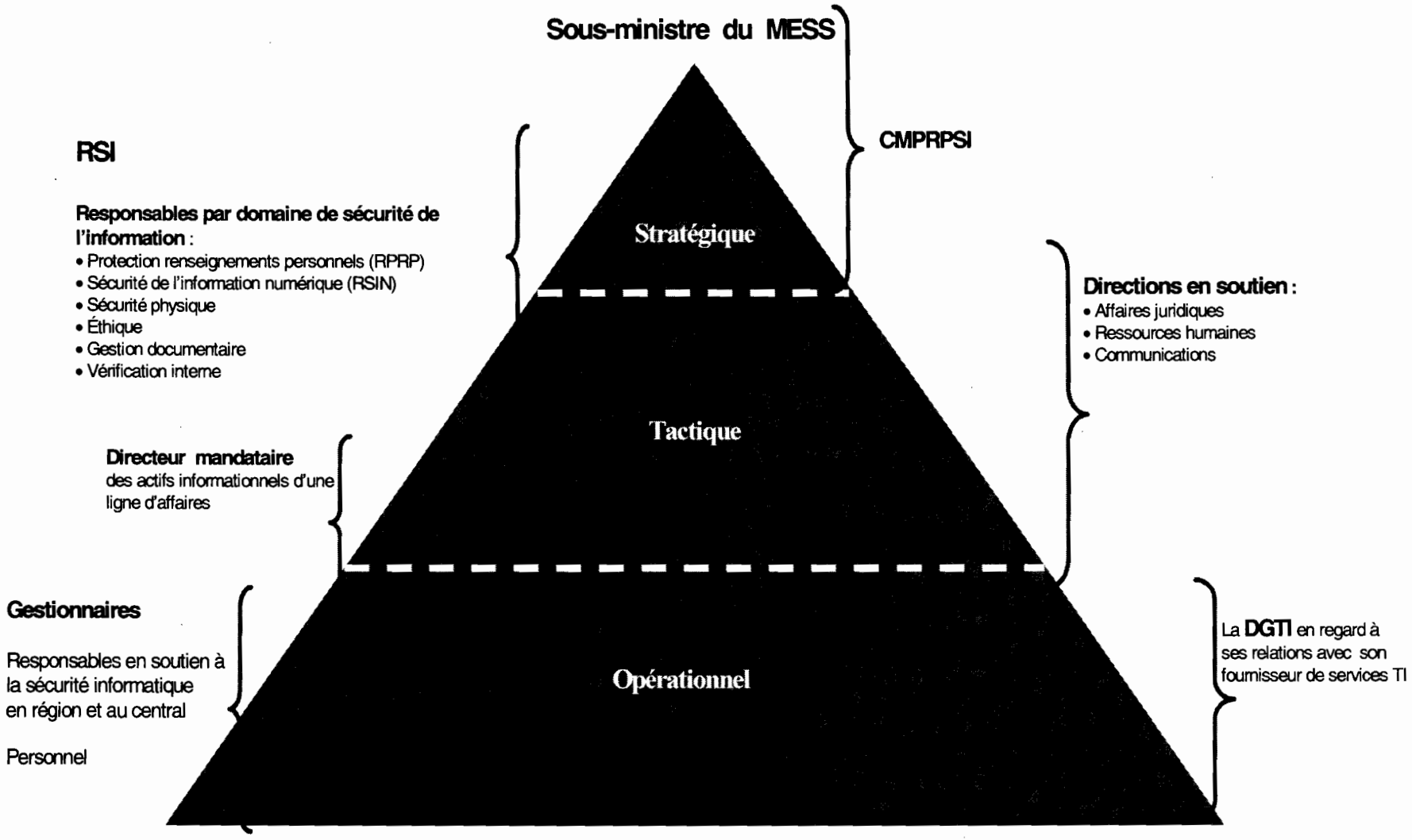
Le **niveau tactique** vise à faire le lien entre les niveaux d'intervention stratégique et opérationnel. Le RSI avec l'aide des responsables par domaine de sécurité, établit la stratégie globale relative à la sécurité de l'information et veille à transformer en moyens et en actions les décisions pour sa mise en œuvre.

Les responsables par domaine collaborent à la gestion de la sécurité de l'information notamment en fournissant l'expertise et en coordonnant leurs efforts. Par domaine, chaque responsable suit son plan d'action visant la mise en œuvre des orientations et s'assure de l'adéquation entre les besoins et les mesures de sécurité.

Le niveau **opérationnel** consiste à réaliser les actions requises pour concrétiser la gestion de la sécurité de l'information et principalement, à mettre en application les mesures de sécurité établies.

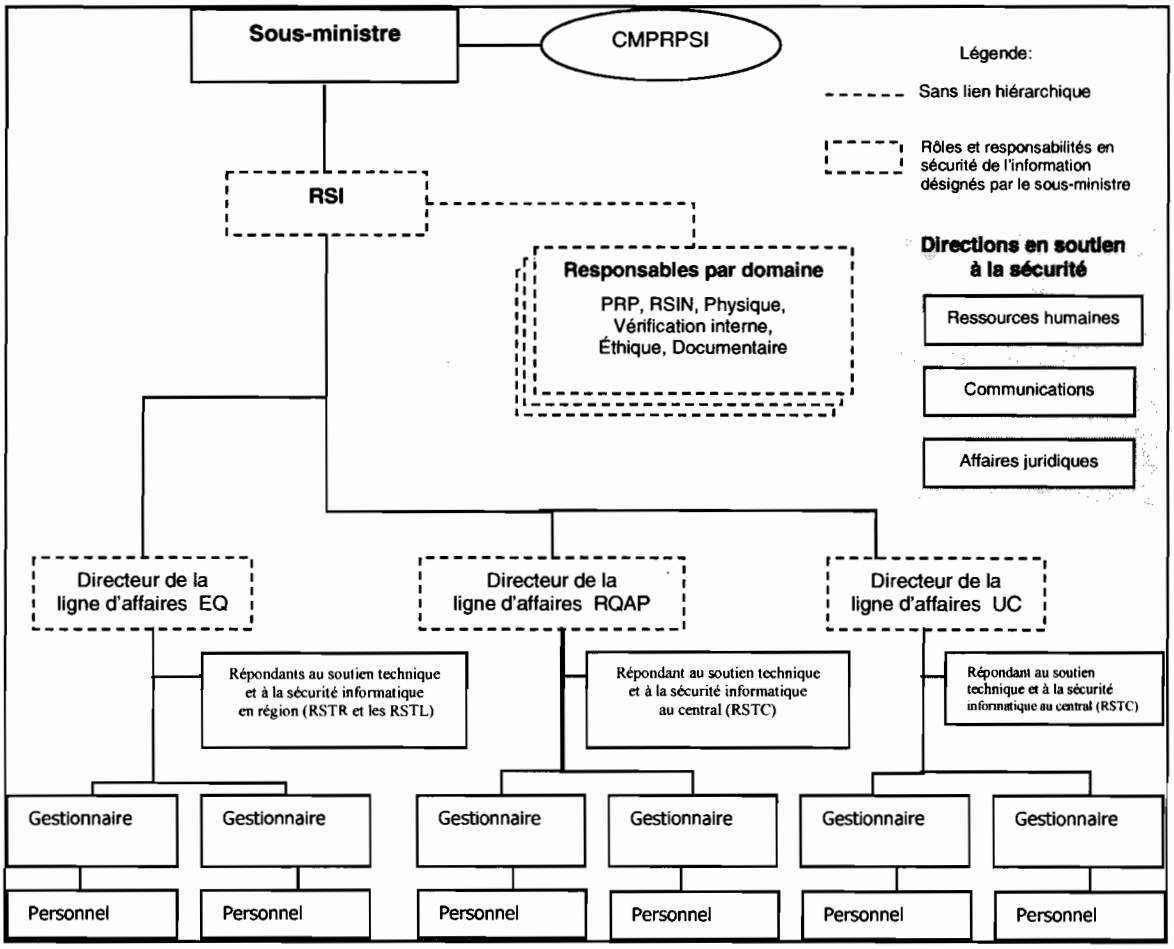
Le schéma suivant positionne les différents intervenants selon leur niveau d'intervention.

[3] **Note au lecteur** : Par souci de lisibilité et pour éviter des changements reliés uniquement aux désignations de nouvelles personnes, le masculin est utilisé comme générique dans ce document.


Sous-ministre du MESS
CMPRPSI
RSI
Responsables par domaine de sécurité de l'information :
• Protection renseignements personnels (RPRP)
• Sécurité de l'information numérique (RSIN)
• Sécurité physique
• Éthique
• Gestion documentaire
• Vérification interne
Stratégique
Directions en soutien :
• Affaires juridiques
• Ressources humaines
• Communications
Tactique
Directeur mandataire
des actifs informationnels d'une ligne d'affaires
Gestionnaires
Responsables en soutien à la sécurité informatique en région et au central
Personnel
Opérationnel
La DGTI en regard à ses relations avec son fournisseur de services TI

5.2 Structure de la gestion de la sécurité

Le schéma suivant présente la structure de gestion de la sécurité de l'information.



6 Rôles et responsabilités

6.1 Le sous-ministre

Le sous-ministre préside le Comité ministériel sur la protection des renseignements personnels et sur la sécurité de l'information (CMPRPSI) mandaté conformément aux obligations énoncées par l'article 2 du Règlement sur la diffusion et sur la protection des renseignements personnels ainsi que celles de l'article 14 de la Directive sur la sécurité de l'information gouvernementale.

Par ailleurs, en matière de gestion de la sécurité de l'information, le sous-ministre est le premier responsable de la sécurité de l'information relevant de son autorité.

À cette fin, il a comme principales responsabilités de :

- En lien avec les valeurs organisationnelles, définir les orientations, les faire partager par l'ensemble de son personnel et les communiquer à ses partenaires ;
- Approuver le cadre normatif et les priorités d'intervention en matière de sécurité de l'information ;
- S'assurer du respect des cadres légaux et normatifs, tant gouvernemental que ministériel ;
- S'assurer de l'application des droits du public en regard de l'accès à l'information et de la protection des renseignements personnels ;
- Gérer les risques ministériels en matière de sécurité de l'information ;
- Présenter, lorsque requis, au ministre des Services gouvernementaux les plans d'action et les bilans demandés;
- Désigner le responsable de la sécurité de l'information (RSI), les responsables par domaine de sécurité de l'information et les mandataires, puis diffuser les désignations au sein du Ministère ;
- Assigner tout autre mandat requis en matière de gestion de la sécurité de l'information.

6.2 Autres intervenants du niveau de la gestion stratégique de la sécurité de l'information du Ministère

Ces autres intervenants ministériels, qui ont des rôles et responsabilités par rapport à la gestion stratégique de la sécurité de l'information du Ministère, sont les suivants :

- Le responsable ministériel de la sécurité de l'information (RSI);
- Le Comité ministériel de la protection des renseignements personnels et de la sécurité de l'information (CMPRPSI).

6.2.1 Le responsable ministériel de la sécurité de l'information (RSI)

Le responsable ministériel de la sécurité de l'information (RSI) représente et assiste le sous-ministre en matière de gestion et de coordination de la sécurité de l'information au Ministère. Il s'assure de maintenir une vision globale de la sécurité de l'information ainsi qu'une cohérence dans la gestion de la sécurité.

Il a comme principales responsabilités de :

- Proposer les orientations et les priorités d'intervention ;
- Gérer au nom du sous-ministre, le processus formel de gestion intégrée et d'amélioration continue de la sécurité de l'information ;
- Proposer une structure de coordination et de concertation où les rôles et responsabilités sont clairement attribués à des personnes identifiées à tous les niveaux de l'organisation ;
- Établir la stratégie globale relative à la sécurité de l'information du Ministère ;
- Gérer la mise en oeuvre du cadre normatif ministériel relatif à la sécurité de l'information ainsi que la mise en application de la présente politique ;
- Suivre les plans d'action par domaine de sécurité ;
- Présenter les plans d'action et les bilans relatifs à la sécurité de l'information qui seront demandés par le sous-ministre ;
- Encadrer la gestion des risques en matière de sécurité de l'information notamment en :
    - s'assurant de l'instauration de mécanismes d'identification et d'évaluation des risques ;
    - s'assurant de l'adéquation des mesures de sécurité en vigueur par rapport à ces derniers.
- Encadrer la gestion des incidents en matière de sécurité de l'information ;
- Participer au processus de continuité des services des différentes lignes d'affaires du Ministère;
- S'assurer de la réalisation de la campagne de sensibilisation des employés à la sécurité de l'information, en outre par la poursuite de la stratégie de communication qui a déjà été élaborée à ce sujet ;
- S'assurer périodiquement de l'actualisation du registre d'autorité de la sécurité de l'information numérique et le faire approuver par le sous-ministre ;
- S'assurer que soient intégrées, dans les ententes avec les partenaires et fournisseurs, les clauses types garantissant le respect des exigences en matière de sécurité de l'information ;
- S'assurer qu'un responsable pour chacun des six domaines de la sécurité de l'information soit assigné, afin de l'appuyer dans ces activités de gestion et de coordination de la sécurité de l'information au Ministère;
- Informer annuellement le CMPRPSI concernant la liste des futurs projets de développement et de refonte de systèmes d'information ou de prestation électronique de services véhiculant des renseignements personnels;

- Mandater, lorsque requis, des groupes de travail relativement à des questionnements spécifiques en matière de sécurité de l'information.

6.2.2 Le Comité ministériel de la protection des renseignements personnels et de la sécurité de l'information (CMPRPSI)

Le CMPRPSI a le mandat de renforcer la protection des renseignements personnels et la sécurité de l'information au sein du ministère de l'Emploi et de la Solidarité sociale.

En matière de sécurité de l'information, il a comme principales responsabilités de :

- Proposer au sous-ministre des orientations stratégiques et les priorités d'intervention en matière de sécurité de l'information ;
- Proposer, au besoin, au sous-ministre des améliorations au cadre normatif ministériel relatif à la sécurité de l'information;
- Participer à la définition de la stratégie globale relative à la sécurité de l'information du Ministère;
- S'assurer de l'intégration des activités de sécurité, découlant de la stratégie globale de la sécurité de l'information, dans les plans d'actions des différentes lignes d'affaires du Ministère;
- S'informer annuellement de la liste des futurs projets de développement et de refonte d'un système d'information ou de prestation électronique de services véhiculant des renseignements personnels;
- Parmi cette liste de projets, préciser ceux qui devront être nécessairement encadrés par les mesures suivantes :
    - la nomination d'une personne chargée de la mise en oeuvre des mesures de protection des renseignements personnels pour le projet, incluant l'évaluation des risques d'atteinte à la protection des renseignements personnels;
    - l'obligation d'identifier les mesures propres à assurer la protection des renseignements personnels pendant toute la période de réalisation du projet ainsi que lors de l'utilisation, de l'entretien, de la modification et de l'évolution du système d'information ou de prestation électronique concerné;
    - l'obligation de décrire les exigences de protection des renseignements personnels dans le cahier de charges ou le contrat relatif au projet, à moins que l'exécutant du contrat soit un autre organisme public;
    - l'obligation de décrire, dans le manuel d'organisation de projet, des responsabilités en matière de protection des renseignements des intervenants ministériels impliqués au projet ;
    - l'obligation de tenir des activités spécifiques de formation sur la protection des renseignements personnels à l'intention des participants au projet.

6.3 Les intervenants du niveau tactique : les responsables des différents domaines de la sécurité de l'information

Les responsables par domaines soutiennent le RSI dans un champ de compétence spécifique. Les domaines sont la protection des renseignements personnels (PRP), la sécurité de l'information numérique (SIN), la sécurité physique, la vérification interne, l'éthique et la gestion documentaire.

6.3.1 Responsable ministériel de l'accès et de la protection des renseignements personnels

Le responsable ministériel de l'accès et de la protection des renseignements personnels (PRP) joue un rôle d'expert-conseil et assiste le sous-ministre dans l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Par ailleurs, en matière de gestion de la sécurité de l'information, le responsable ministériel de l'accès et de la PRP participe aux mécanismes de coordination et de concertation en sécurité et collabore avec le RSI.

À cette fin, il a comme principales responsabilités de :

- Gérer le volet « protection des renseignements personnels » du cadre normatif ministériel relatif à la sécurité de l'information;
- Exprimer les préoccupations ministérielles en matière de PRP ;
- Identifier les risques qui peuvent venir menacer la protection des renseignements personnels (PRP);
- Émettre des avis relatifs à la PRP et transmettre copie de cet avis aux responsables des autres domaines, lorsque l'avis comporte des aspects liés à leur champ de compétence;
- Collaborer aux activités de sensibilisation des employés à la sécurité de l'information;
- Participer à l'élaboration et au suivi de l'application de la procédure de déclaration systématique des incidents en PRP et en sécurité de l'information.

6.3.2 Responsable de la sécurité de l'information numérique du Ministère (RSIN)

En matière de sécurité de l'information numérique, le RSIN du MESS participe aux mécanismes de coordination et de concertation en sécurité et collabore avec le RSI dans l'exercice de ses fonctions.

Il a comme principales responsabilités de :

- Gérer le volet « sécurité numérique » du cadre normatif ministériel relatif à la sécurité de l'information;
- Exprimer les préoccupations ministérielles en matière de sécurité de l'information numérique ;
- Proposer au RSI des orientations, un plan d'action concernant son domaine d'intervention et lui soumettre annuellement un bilan des actions réalisées;
- Identifier les risques qui peuvent venir menacer la protection de l'information numérique ;

- Émettre des avis de sécurité visant à conseiller les mandataires sur les mesures à mettre en place en vue de protéger leur information numérique et transmettre copie de cet avis aux responsables des autres domaines, lorsque l'avis comporte des aspects liés à leur champ de compétence;
- Collaborer aux activités de sensibilisation des employés à la sécurité de l'information;
- Participer à l'élaboration et au suivi de l'application de la procédure de déclaration systématique des incidents en PRP et en sécurité de l'information.

6.3.3 Direction de la gouverne des technologies de l'information (DGTI)

En regard de la sécurité des technologies de l'information (TI) supportant les actifs informationnels du Ministère et à titre de donneur d'ouvrage dans un contexte d'impartition des services en TI rendus au Ministère, la DGTI doit s'assurer que son principal fournisseur de services, soit la vice-présidence des technologies de l'information (VPTI) du CSPQ, lui fournisse les services en cette matière suivants :

- Procéder à l'élaboration et à la diffusion des pratiques et mesures de sécurité relatives à l'utilisation sécuritaire des technologies de l'information utilisées par le Ministère;
- Soutenir les utilisateurs du MESS par rapport à l'interprétation et l'application de ces pratiques et mesures de sécurité;
- Informer le RSIN du MESS relativement aux incidents qui ont mis ou ont pu mettre en péril la sécurité des informations du Ministère véhiculées par les technologies de l'information du CSPQ et voir à appliquer les actions requises pour leur résolution;
- Aviser le RSIN du MESS sur les risques informatiques encourus dans l'utilisation des technologies de l'information du CSPQ versus le niveau de protection de l'information numérique attendu du Ministère;
- Assurer la mise en place des mesures de sécurité appropriées au cours des futurs projets d'évolution ou de développement de systèmes informatiques demandés par le MESS et informer le gestionnaire mandataire concerné sur les risques résiduels possibles.

6.3.4 Responsable de la sécurité physique

Le responsable de la sécurité physique (RSP) a pour objectif d'assurer la protection, grâce à la mise en œuvre des moyens techniques appropriés, de l'information détenue au Ministère, de la confidentialité des renseignements personnels, du personnel lui-même et de l'équipement.

Par ailleurs, en matière de gestion de la sécurité de l'information, le RSP participe aux mécanismes de coordination et de concertation en sécurité et collabore avec le RSI dans l'exercice de ses fonctions.

Il a comme principales responsabilités de :

- Gérer le volet « sécurité physique » du cadre normatif ministériel relatif à la sécurité de l'information, dont la Politique ministérielle sur la sécurité physique dans les édifices du MESS ;
- Exprimer les préoccupations ministérielles en cette matière ;
- Proposer au RSI des orientations, un plan d'action concernant son domaine d'intervention et lui soumettre annuellement un bilan des actions réalisées;
- Évaluer les risques matériels qui peuvent venir menacer la sécurité de l'information ministérielle ;

- Émettre des avis de sécurité sur les mesures de sécurité physique à mettre en place ;
- Collaborer aux activités de sensibilisation des employés à la sécurité de l'information;
- Traiter les incidents relatifs à la sécurité physique ;
- Participer à l'élaboration et au suivi de l'application de la procédure de déclaration systématique des incidents en PRP et en sécurité de l'information.

6.3.5 Responsable de la gestion documentaire

Le responsable de la gestion documentaire assiste, en sécurité de la gestion documentaire, le responsable ministériel de la sécurité de l'information (RSI).

Il a comme principales responsabilités de :

- Gérer le volet « gestion documentaire » du cadre normatif ministériel relatif à la sécurité de l'information;
- Exprimer les préoccupations ministérielles en cette matière ;
- Produire au RSI des orientations, un plan d'action concernant son domaine d'intervention et lui soumettre annuellement un bilan des actions réalisées;
- Participer à l'évaluation des risques relatifs à la gestion documentaire appliquée au Ministère;
- Participer aux mécanismes de coordination et de concertation en sécurité et exprimer ses préoccupations ;
- Participer aux activités de sensibilisation des employés à la sécurité de l'information et qui sont relatives à la gestion documentaire;
- Gérer le calendrier de conservation et s'assurer de son application en ce qui concerne les actifs informationnels ;
- Soutenir les mandataires dans leurs activités de gestion documentaire.

6.3.6 Responsable ministériel en éthique

Le responsable ministériel en éthique a pour mandat d'implanter et de soutenir dans son ministère une culture éthique.

Par ailleurs, en matière de gestion de la sécurité de l'information, le responsable ministériel en éthique participe aux mécanismes de coordination et de concertation en sécurité et assiste le RSI dans l'exercice de ses fonctions.

Il a comme principales responsabilités de :

- Promouvoir le volet « éthique » du cadre normatif ministériel relatif à la sécurité de l'information;
- Exprimer les préoccupations ministérielles en cette matière ;
- Participer aux mécanismes de coordination et de concertation en sécurité et exprimer ses préoccupations ;
- Émettre des avis lorsque des règles déontologiques en matière de sécurité doivent être établies ;

- Évaluer l'application des considérations éthiques en regard à l'utilisation faite par les employés des technologies de l'information mises à leur disposition ;
- Collaborer aux activités de sensibilisation des employés à la sécurité de l'information.

6.3.7 Responsable de la vérification interne et des enquêtes administratives

Le responsable de la vérification interne et des enquêtes administratives supporte la haute direction quant à son degré de contrôle sur les systèmes, processus et activités.

Par ailleurs, il participe aux mécanismes de coordination et de concertation en sécurité de l'information, collabore avec le RSI dans l'exercice de ses fonctions et contribue à la reddition de comptes en matière de sécurité de l'information.

Il a comme principales responsabilités de :

- S'assurer que la Politique ministérielle en matière de vérification interne tient compte de la sécurité de l'information du Ministère ;
- Conseiller les gestionnaires dans le développement de leurs actifs informationnels en regard aux contrôles à appliquer par ces derniers ;
- Agir à titre de rôle conseil dans la définition des règles de journalisation, des règles d'accès et les délais de conservation des journaux applicatifs de ces derniers;
- Évaluer, au besoin, l'efficacité et l'efficience des activités de contrôle et de gestion des risques appliquées en matière de gestion de la sécurité de l'information au Ministère;
- Effectuer des enquêtes suite à la demande des gestionnaires et/ou suite à la détection de l'usage illicite ou abusif des données informationnelles ainsi que des outils informatiques mis à la disposition du personnel ;
- Répondre aux demandes de vérification de sécurité avant nomination de chaque nouvel employé ministériel dont l'emploi sera considéré à risque en regard à la sécurité de l'information du Ministère ;
- Participer à titre de rôle conseil à la mise en place de la campagne de sensibilisation des employés à la sécurité de l'information.

6.4 Les intervenants au niveau opérationnel

6.4.1 Les directeurs mandataires d'actifs informationnels d'une ligne d'affaires

Le directeur d'une ligne d'affaires est le mandataire du processus et de tous les actifs informationnels qui soutiennent ses activités. À cet égard, il aura à s'assurer que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement, et ce, tout au long du cycle de vie de ses actifs. Le mandataire est désigné par le sous-ministre et son nom est consigné dans le registre d'autorité.

Ses principales responsabilités à l'égard de ses actifs informationnels sont de :

- S'assurer du respect des exigences légales et normatives en matière de sécurité de l'information dès la conception et durant tout le cycle de vie de l'information ;

- Gérer le processus de l'identité et des droits d'accès relatifs aux actifs informationnels de sa ligne d'affaires;
- Autoriser et répondre de l'utilisation de ses actifs informationnels;
- S'assurer que les contrôles adéquats concernant ses actifs informationnels sont appliqués;
- Déterminer les risques et le niveau de protection requis ;
- Prendre en charge les mesures de sécurité :
    - en veillant à ce que les mesures de sécurité appropriées concernant ses actifs informationnels soient mises en place, appliquées et périodiquement vérifiées ;
    - en s'assurant de l'adéquation des mesures par rapport au niveau de protection requis;
- Désigner une personne responsable de préciser les exigences en matière de protection des renseignements personnels, pour tout projet de développement ou de refonte d'un système d'information ou de prestation électronique de services véhiculant des renseignements personnels, et en informer le responsable ministériel de l'accès et de la PRP;
- Réaliser la catégorisation de chaque nouveau système d'information en tant qu'actif informationnel à être inscrit ultérieurement au registre d'autorité ;
- Communiquer, au responsable ministériel de l'accès et de la protection des renseignements personnels, l'existence de tous les actifs contenant des renseignements personnels ;
- Organiser le processus de gestion de la continuité des services de sa ligne d'affaires ;
- Produire annuellement un état de situation de la sécurité de ses actifs informationnels ;
- S'assurer que ses employés clés, c'est-à-dire les pilotes de systèmes, reçoivent une formation adéquate en sécurité de l'information ;
- Participer aux mécanismes de coordination et de concertation en sécurité ;
- S'assurer d'intégrer, dans les ententes avec les partenaires et fournisseurs, les clauses garantissant le respect des exigences de sécurité ;
- S'assurer de la prise des décisions nécessaires au cours de la résolution de tout incident venant affecter la sécurité de l'un de ses actifs informationnels.

6.4.2 Les gestionnaires

Le gestionnaire assume des responsabilités en matière de sécurité au sein de son unité administrative. Il a comme principales responsabilités de :

- Agir comme mandataire pour les informations propres à son unité administrative conservées dans des actifs informationnels développés en milieu utilisateur et informer le responsable ministériel de l'accès et de la PRP concernant l'existence de ces actifs lorsqu'ils contiennent des renseignements personnels ;
- S'assurer de l'application par son personnel des mesures de sécurité de l'information qui ont été mises en place;
- Aviser dès que connus des mouvements de personnel dans son unité administrative ;

- Gérer les demandes d'accès aux systèmes du Ministère pour les différents intervenants relevant de son autorité (personnel, clients, mandataires, partenaires ou fournisseurs) ;
- S'assurer que les accès restent en tout temps conformes aux besoins et aux tâches de l'intervenant ;
- S'assurer que les employés de son unité administrative connaissent leurs responsabilités en matière de sécurité de l'information ;
- S'assurer d'intégrer, dans les ententes avec ses partenaires et fournisseurs, les clauses garantissant le respect des exigences de sécurité ;
- Signaler tout incident qui met ou a pu mettre en péril la sécurité de l'information en fonction des procédures en vigueur au Ministère.

6.4.3 Le personnel

Le personnel assume comme principales responsabilités de :

- Respecter les exigences légales et normatives en matière de sécurité de l'information et de PRP;
- Appliquer les mesures de sécurité établies pour assurer la sécurité de l'information[4] ;
- N'utiliser l'information qu'aux seules fins prévues ;
- Ne pas communiquer ou divulguer de renseignements auxquels il a accès, à moins que cette communication ou cette divulgation ne soit autorisée par la loi ou prévue dans une entente ;
- Ne prendre connaissance que de l'information liée aux dossiers qui lui sont assignés et à ne divulguer les faits ou les renseignements obtenus dans l'exercice de ses fonctions que s'il est autorisé par la loi ;
- Adopter un comportement éthique[5] dans l'utilisation des technologies de l'information mises à sa disposition;
- Adhérer à ce que ses accès restent en tout temps conformes à ses besoins et à ses tâches ;
- Rapporter à son gestionnaire tout incident qui met ou a pu mettre en péril la sécurité de l'information détenue par le Ministère.

6.4.4 Les répondants au soutien technique et à la sécurité informatique

Ces personnes, oeuvrant pour le compte du Ministère, assument la responsabilité suivante :

- Accomplir des activités de soutien relatives à l'application des mesures de sécurité de l'information par les employés du Ministère travaillant dans leur région ou leur unité administrative au central;
- S'assurer de la mise en œuvre des mesures appropriées de sécurité informatique et de protection des renseignements personnels dans leur développement d'applications en milieu utilisateur (DMU);

[4] Ces mesures émanent des responsables des différents domaines de la sécurité de l'information, de consignes émises par les gestionnaires mandataires des actifs informationnels ainsi que des lignes directrices émises par le cadre normatif ministériel relatif à la sécurité de l'information.

[5] Se référer aux *Lignes directrices ministérielles sur l'utilisation et la gestion du réseau Internet et du courrier électronique.*

- S'informer préalablement, auprès de leur répondant régional à l'accès aux documents et à la protection des renseignements personnels, par rapport à l'évaluation du niveau de protection requis des renseignements personnels qui seraient véhiculés par ces applications en milieu utilisateur.

6.5 Unités administratives agissant en soutien

Même si elles ne sont pas directement concernées par le processus de gestion de la sécurité de l'information, ces unités administratives sont appelées à soutenir le RSI à même la livraison de leurs offres de services régulières.

6.5.1 La Direction des affaires juridiques

La Direction des affaires juridiques conseille le Ministère sur l'application des lois et des règlements ayant une incidence sur la sécurité de l'information et sa gestion.

En matière de sécurité de l'information, elle a comme principales responsabilités de :

- Participer aux mécanismes de coordination et de concertation de sécurité ;
- Donner des avis concernant l'application des lois et des règlements ;
- Conseiller sur les aspects juridiques au moment de l'élaboration des ententes.

6.5.2 La Direction des ressources humaines

La Direction des ressources humaines soutient le Ministère dans les activités relatives à la gestion du personnel.

En matière de sécurité de l'information, elle a comme principales responsabilités de :

- Soutenir le Ministère dans l'élaboration du matériel de sensibilisation et de formation à la sécurité de l'information ;
- Appliquer les mesures disciplinaires ou les sanctions appropriées à la lumière des résultats des enquêtes administratives ou vérifications de conformité effectuées par la Direction de la vérification interne et des enquêtes administratives ;
- S'assurer que la sécurité est prise en compte dans les procédures internes de gestion des ressources humaines notamment lors de l'embauche, la cessation, le mouvement de personnel.

6.5.3 La Direction des communications

La Direction des communications soutient le Ministère dans les activités de communication. En matière de sécurité de l'information, il a comme principales responsabilités de :

- Poursuivre, en collaboration étroite avec le Responsable ministériel de la sécurité de l'information (RSI) et les responsables des domaines de la sécurité, la campagne de sensibilisation des employés à la sécurité de l'information ;
- Soutenir le Ministère dans l'élaboration et la diffusion du matériel de communication relativement à la sensibilisation des employés à la sécurité de l'information ;
- Coordonner les communications auprès de la population et des médias lors d'incidents majeurs et médiatisés.

7 Dispositions générales

7.1 Modalités de révision

La présente politique sera révisée périodiquement, suite à tout changement important affectant son contexte, afin d'en assurer son adéquation continue aux futures orientations en matière de sécurité de l'information qui seraient éventuellement énoncées par les autorités du Ministère.

De plus, elle remplace l'ancienne politique s'appliquant au «domaine de la gestion de la sécurité de l'information numérique et des échanges électroniques» qui avait été adoptée en mai 2000.

7.2 Date d'entrée en vigueur

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

Original signé par

_____, _____

François Turenne — date

Sous-ministre

ANNEXES

ANNEXE A : DÉFINITIONS

Domaines

Les domaines de la sécurité sont les champs d'intervention en matière de la sécurité de l'information. Ces domaines sont gérés par des unités administratives généralement distinctes. Le tableau présente les domaines identifiés au Ministère et les unités administratives qui les gèrent.

Domaines	Unités administratives responsables
Protection des renseignements personnels	Bureau du sous-ministre (BSM)
Éthique	DRH, Service de la santé des personnes et des politiques (SSPP)
Sécurité de l'information numérique	Direction de la gouverne des TI (DGTI)
Sécurité physique	Direction de la gestion des espaces et des services auxiliaires (DGESA)
Gestion documentaire	Direction de la gestion des espaces et des services auxiliaires (DGESA)

Actifs informationnels

Inventaire présentant, à un moment déterminé, le portrait de l'ensemble des ressources informationnelles d'une entreprise ou d'une organisation, à l'exception des ressources humaines. (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec)

Cadre de gestion

Structure organisationnelle de sécurité de l'information où les rôles et les responsabilités sont attribués à des personnes identifiées à tous les niveaux de l'organisation. (source: Directive sur la sécurité de l'information gouvernementale)

Ensemble des moyens mis en œuvre pour soutenir la prise de décision en vue de l'atteinte des objectifs. (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec)

Cycle de vie de l'information

Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation du ministère ou de l'organisme. (source: Directive sur la sécurité de l'information gouvernementale)

Directive sur la sécurité de l'information gouvernementale

Directive gouvernementale qui détermine la ligne de conduite à adopter, l'orientation à suivre ou la façon de procéder afin d'assurer la cohérence et la coordination des interventions en matière de gestion de la sécurité de l'information gouvernementale. Adoptée par une décision du Conseil du trésor datant du 11 avril 2006 (C.T. 203560), suite à une proposition du ministre des Services gouvernementaux (MSG), cette Directive gouvernementale est entrée en vigueur le 1er mai 2006. Elle remplace la Directive gouvernementale sur la sécurité de l'information numérique et des échanges électroniques dans l'administration (C.T. 194055) qui était entrée en vigueur le 4 février 2000.

Document

Ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ses formes ou en un autre système de symboles.

Est assimilée à la notion de document : toute banque d'information de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. (source: Directive sur la sécurité de l'information gouvernementale)

Mesure de sécurité

Moyen concret qui assure, partiellement ou totalement, la protection de l'actif informationnel contre une ou plusieurs menaces, et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces menaces ou à minimiser les pertes qui en résultent. (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec)

Politique

Ensemble de principes généraux indiquant la ligne de conduite adoptée par une organisation privée ou publique, dans un secteur donné, et qui guident l'action ou la réflexion dans la gestion de ses activités. (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec)

Politique cadre de gestion de la sécurité de l'information

Document qui présente les orientations et principes généraux en matière de sécurité de l'information qu'entend appliquer une organisation ainsi que la description des rôles et responsabilités attribués aux personnes concernées à tous les niveaux de sa structure organisationnelle.

Procédure

Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche. Elle constitue un guide pour l'action en indiquant de quelle façon exécuter une tâche. (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec)

Processus

Ensemble d'activités logiquement interreliées qui produisent un résultat déterminé. (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec)

Registre d'autorité de la sécurité

Document qui présente les délégations consenties aux fins de la gestion de la sécurité de l'information. Il inventorie les actifs informationnels ainsi que leur mandataire.

Ressources informationnelles

Ressource utilisée par une entreprise ou une organisation, dans le cadre de ses activités de traitement de l'information, pour mener à bien sa mission, pour la prise de décision, ou encore pour la résolution de problèmes. Une ressource informationnelle est généralement un système d'information qui est utilisé relativement 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 la destruction des éléments d'information. Une ressource informationnelle peut aussi être uniquement le fichier ou la banque de données d'un progiciel informatique utilisé en service externe (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec).

Risque

Probabilité que survienne un événement nuisible et éventualité qu'existe une menace plus ou moins prévisible pouvant influer sur la réalisation des objectifs d'une organisation. (source: Grand dictionnaire terminologique de l'Office de la langue française du Québec).

Sécurité de l'information

Ensemble des moyens technologiques, humains, organisationnels, juridiques et éthiques permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information.