Politique
de sécurité de l'information

Québec

Politique

de sécurité
de l'information

Québec

La Politique de sécurité de l'information a été préparée
par la Direction générale des services à la gestion
du ministère des Transports du Québec.
Elle a été éditée par la Direction des communications.

Dépôt légal
Bibliothèque nationale du Québec 2004
ISBN 2-550-42202-3

Table des matières

1 Introduction

Le 4 février 2000, le Conseil du trésor a mis en vigueur la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale (C.T. 194055).

L'ensemble des ministères et des organismes publics du Québec recueillent, conservent, utilisent et disposent, sous forme numérique, des informations nécessaires à la réalisation de leur mission. Ces renseignements peuvent être de nature confidentielle ou sensible. Ils peuvent présenter une valeur légale, administrative, économique ou patrimoniale. Et, par conséquent, ils doivent être adéquatement protégés. Toute l'information détenue par le ministère des Transports constitue donc une ressource essentielle, dont il convient d'assurer la sécurité en tout temps.

La directive C.T. 194055 établit que les ministères et les organismes sont les premiers responsables de la sécurité de l'information numérique qu'ils détiennent ou utilisent ainsi que de la sécurité des échanges électroniques qu'ils réalisent. Le Ministère doit donc élaborer un ensemble de mesures qui lui permettront de gérer les risques et leurs effets sur la disponibilité, l'intégrité, la confidentialité de son information, ainsi que sur l'authentification des utilisateurs et l'irrévocabilité des documents qu'ils rédigent ou des actions qu'ils mènent.

C'est donc en conformité avec la directive précitée que le Ministère a entrepris la révision de la Politique de sécurité de l'information, adoptée en 1999. La politique révisée sera intégrée au Plan global de gestion de la sécurité de l'information du Ministère. Outre la politique, le Plan global comprendra un Cadre de gestion de la sécurité de l'information de même qu'une Architecture de la sécurité de l'information numérique (ASIN).

2 Contexte

Le succès de la mission du ministère des Transports est fondé, entre autres, sur le climat de confiance établi avec la population, avec ses mandataires et ses partenaires ainsi qu'avec ses fournisseurs. Ce climat de confiance, qui est essentiel, repose notamment sur la confidentialité des informations obtenues et détenues en conformité avec le cadre légal et réglementaire en vigueur au Québec.

Conscient de la valeur de l'information qu'il détient ou qu'il utilise, le Ministère a la responsabilité d'en assurer la protection. Cette responsabilité rend donc nécessaire la mise en œuvre d'un plan global de gestion de la sécurité de l'information, que vient soutenir la présente politique.

3 Domaine d'application

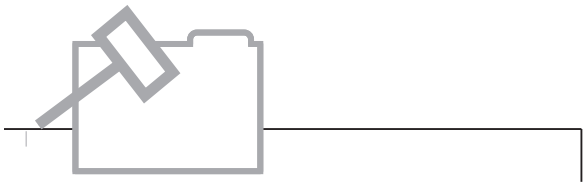
La politique ministérielle s'applique aux ressources informationnelles[1] détenues ou utilisées par l'ensemble des unités administratives du ministère des Transports, et ce, tout au long de leur cycle de vie et sans égard à leur localisation.

La politique s'applique à toute personne qui travaille pour le Ministère et a accès à une ressource informationnelle détenue ou utilisée par ce dernier, et ce, sans égard au statut d'emploi (personnel régulier, occasionnel ou contractuel). De plus, les mandataires, partenaires et fournisseurs sont soumis aux mêmes obligations que le personnel lorsqu'ils accèdent aux ressources informationnelles appartenant au Ministère ou qu'ils les utilisent.

Toutes les activités impliquant la manipulation ou l'utilisation, sous quelque forme que ce soit, des ressources informationnelles du Ministère sont visées par la présente politique, qu'elles soient effectuées dans ses locaux, dans un autre lieu ou à distance. En outre, cette politique s'applique dès l'étape de la conception d'une ressource informationnelle ainsi que pendant la réalisation ou la modification d'un processus d'affaires, d'un système d'information ou d'une infrastructure technologique.

1. Ressources informationnelles : actifs informationnels et 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.

4 Cadre juridique et normatif



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

- le Code civil du Québec (L.Q., 1991, c.64), notamment les articles 36 et 37, qui portent respectivement sur le respect de la vie privée et la communication des renseignements confidentiels;
- le Code criminel du Canada (L.R.C., 1985, c. C-46), notamment les articles 342.1, 366 et 430, qui portent respectivement sur l'interception frauduleuse d'informations, la falsification des documents et les méfaits;
- la Loi sur le droit d'auteur (L.R.C., 1985, c. C-42);
- la Loi sur les marques de commerce (L.R.C., 1985, c. T-13);
- la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);
- la Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12) et la Charte canadienne des droits et libertés, Annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R-U);
- 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 Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, c. 5);
- la Loi sur les archives (L.R.Q., c. A-21.1), en ce qui a trait aux exigences relatives à la protection et à la conservation des documents ayant une valeur patrimoniale ou archivistique;
- la Loi sur la fonction publique (L.R.Q., c. F-3.1.1), notamment les articles 4 à 9, et plus particulièrement les dispositions du Règlement sur les normes d'éthique, de discipline et le relevé provisoire des fonctions dans la fonction publique traitant des normes d'éthique et de discipline dans la fonction publique québécoise;
- la Loi sur l'administration publique (L.R.Q., c.A-6.01), un nouveau cadre de gestion pour la fonction publique;
- le Règlement sur l'éthique et la déontologie des administrateurs publics, Loi sur le ministère du Conseil exécutif (L.R.Q., c. M-30, a. 3.0.1 et 3.0.2, 1997, c. 6, a. 1);
- les Normes en matière d'acquisition, d'utilisation et de gestion des droits d'auteur des documents détenus par le gouvernement et les ministères et organismes désignés, en vigueur depuis le 1er novembre 2000 (A.M., 2000 : Gazette officielle du Québec, 25 octobre 2000, p.6753);
- la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale (C.T. 194055 du 23 novembre 1999);
- la Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique (Loi sur l'administration publique - L.R.Q., c. A-6.01, a. 31), (C.T. 198872 du 1er octobre 2002);

- le Cadre de gestion des ressources informationnelles en soutien à la modernisation de l'Administration publique (C.T. 197638 du 29 janvier 2002).

Ont également été prises en considération les lois encadrant la mission du ministère des Transports, notamment :

- la Loi sur le ministère des Transports (L.R.Q., c. M-28);
- la Loi sur la voirie (L.R.Q., c. V-9);
- la Loi sur les transports (L.R.Q., c. T-12).

5 Énoncé de la politique

Dans le but d'atteindre ses objectifs de sécurité, le Ministère énonce des lignes directrices, qui sont conformes aux orientations gouvernementales et qui constituent le fondement des règles, procédures, normes et autres mesures de sécurité nécessaires pour assurer la protection de ses ressources informationnelles.

La réalisation de la mission ministérielle

Les ressources informationnelles du Ministère sont essentielles à la réalisation de ses activités et doivent faire l'objet d'une utilisation et d'une protection adéquates. La sécurité de l'information contribue à la réalisation de la mission du ministère des Transports et au maintien de la confiance de la population à l'égard des services publics. Le niveau de protection accordé est fonction de la sensibilité des ressources et des risques d'accidents, d'erreurs et de malveillance auxquels elles sont exposées.

La vision commune

L'atteinte d'un niveau de sécurité adéquat nécessite l'adhésion à une vision et à une compréhension communes de la sécurité et doit s'appuyer sur l'implication continue de tous les gestionnaires et de tous les utilisateurs.

La cohérence

La sécurité doit reposer sur une approche globale et intégrée qui tienne compte des aspects juridique, humain, organisationnel et technologique. Elle demande la mise en œuvre d'un ensemble de mesures coordonnées de prévention, de détection, de correction et de sanction.

La responsabilité et l'imputabilité

L'efficacité des mesures de sécurité exige que les responsabilités soient clairement définies, à tous les niveaux de l'organisation, et que soient adoptés des mécanismes de coordination et de contrôle permettant une reddition de comptes adéquate.

L'évolution

Les pratiques et solutions techniques adoptées par le Ministère doivent être réévaluées périodiquement afin de tenir compte des changements organisationnels et technologiques ainsi que de l'évolution de la menace et des risques.

L'universalité

Les pratiques et solutions techniques adoptées doivent correspondre, dans la mesure du possible, aux manières de faire reconnues et utilisées à l'échelle nationale et internationale.

La protection des renseignements confidentiels et sensibles

Toute information considérée confidentielle ou sensible doit être protégée contre l'accès ou les utilisations 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 les renseignements 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.

La continuité des affaires

Le Ministère doit prévoir des mesures d'urgence, consignées par écrit et éprouvées, en vue d'assurer la remise en fonctionnement, dans un délai raisonnable, des systèmes d'information jugés essentiels, en cas de sinistre majeur, et ce, dans le respect de ses obligations relatives à la Loi sur la sécurité civile.

À cet égard, le Ministère dispose d'un plan de reprise informatique qui constitue une composante essentielle de son plan global de gestion de la sécurité, prévoyant tous les cas possibles d'arrêt de fonctionnement des ressources informatiques, de même que toutes les mesures applicables à chacun de ces cas, afin que puisse être assurée la continuité des services informatiques.

La sensibilisation et la formation

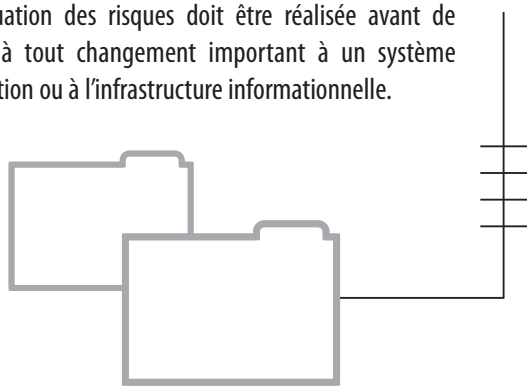
Chaque gestionnaire doit sensibiliser son personnel à la sécurité des ressources informationnelles, aux conséquences d'une atteinte à la sécurité ainsi qu'au rôle et aux responsabilités de tous les employés de son unité administrative dans la protection des ressources. Le gestionnaire doit également veiller à ce que le personnel directement engagé dans les processus assurant la sécurité ministérielle ait reçu une formation relative aux mécanismes, aux solutions technologiques et aux mesures de sécurité.

La catégorisation des actifs informationnels

Chaque actif informationnel du Ministère doit être catégorisé par son détenteur et protégé selon son niveau de confidentialité et les exigences qui y sont liées en fait de disponibilité, d'intégrité, d'authentification et d'irrévocabilité.

L'évaluation des risques

Le choix des mesures de sécurité protégeant un actif informationnel doit s'appuyer sur une évaluation de la menace et des risques, notamment d'accès non autorisés, d'atteinte à l'intégrité ou à la disponibilité de l'information. En outre, une évaluation des risques doit être réalisée avant de procéder à tout changement important à un système d'information ou à l'infrastructure informationnelle.



La gestion des preuves non informatiques

Dans le but d'assurer la gestion des preuves non informatiques, le traitement ou la manipulation d'une information ne doit pas en altérer l'intégrité. Dans ce contexte, l'intégrité des ressources informationnelles, et en particulier de l'information et des documents technologiques du Ministère est garantie entre autres par les mesures de sécurité physique prises pour les protéger. Le maintien de l'intégrité d'un document permet d'en conserver la valeur juridique et de le rendre admissible en preuve devant les tribunaux.

Qu'il s'agisse de copier un document, de le transmettre ou de le transférer d'un support à un autre, son intégrité et, conséquemment, sa valeur probante sont évaluées en fonction de la fiabilité du procédé utilisé et des mesures de contrôle entourant l'ensemble de la procédure. Les caractéristiques techniques permettant de conclure à cette fiabilité sont décrites dans une documentation associée aux systèmes de traitement, de copie ou de transmission, ou encore elles sont jointes aux documents transférés sur un autre support.

Aux mêmes fins, et pour assurer l'intégrité de ses documents technologiques pendant la période où ils doivent être préservés, le Ministère doit autoriser préalablement toute modification et en conserver les paramètres.

Le droit de regard

Le Ministère a un droit de regard sur l'utilisation de ses ressources informationnelles, qui sera exercé conformément à la législation en vigueur et dans le respect de la vie privée des utilisateurs.

Ces lignes directrices en matière de sécurité de l'information visent à établir une saine gestion des risques et de leurs effets à l'égard de [2] :

- la disponibilité, qui est le fait pour une information d'être accessible en temps voulu et de la manière requise par les personnes autorisées;
- l'intégrité, qui est l'état d'une information ou d'une technologie de l'information qui n'a été ni modifiée ni détruite;
- la confidentialité, qui est le fait pour une information de n'être accessible qu'aux personnes autorisées;
- l'authentification, qui est l'acte par lequel on établit l'identité d'une personne ou d'un dispositif;
- l'irrévocabilité, qui est le fait pour une action ou un document d'être irréfutable et de pouvoir être clairement attribué à son auteur ou au dispositif qui l'a généré;
- l'habilitation / le contrôle des accès, qui consiste à établir une liste des ressources informationnelles auxquelles une personne ou un dispositif peut accéder après avoir été dûment identifié;
- la surveillance, qui sert à déceler les lacunes, à proposer des pistes pour la vérification et à protéger contre les tentatives d'intrusion et les programmes malicieux;
- l'administration, qui est responsable de la sécurité des logiciels et des équipements informatiques et de réseautique; elle comprend à la fois les processus, tels que la réalisation du schéma de configuration, l'inventaire et la tenue des dossiers,et les outils.

2 Comme il est mentionné dans la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale, les exigences DICAI en matière de sécurité se définissent en termes de disponibilité, d'intégrité, de confidentialité, d'authentification et d'irrévocabilité. L'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) ajoute, quant à elle, trois nouvelles exigences aux cinq précédentes, soit l'habilitation/le contrôle des accès, la surveillance et l'administration.

6 Règles administratives en matière de sécurité

Dans le cadre de la mise en œuvre de l'Architecture de la sécurité de l'information numérique (ASIN), le ministère des Transports s'est doté d'un ensemble de règles relatives à l'administration sécuritaire de l'infrastructure technologique ministérielle[3].

Ces règles doivent guider l'administration générale de l'infrastructure technologique ministérielle, notamment du réseau ministériel, et ce, dans le respect de la présente politique. De ces règles administratives découlent des règles particulières relatives à l'élaboration, l'exploitation et l'utilisation sécuritaire des composantes de l'infrastructure technologique ministérielle.

Les règles administratives doivent donc être conçues et appliquées dans le but de répondre adéquatement aux exigences DICAI en matière de sécurité, et ce, en fonction de la sensibilité des ressources informationnelles et des risques d'accidents, d'erreurs et de malveillance auxquels elles sont exposées. Ainsi, les besoins en matière de sécurité doivent être définis en évaluant les risques et en déterminant si les mesures de sécurité déjà en vigueur sont suffisantes.

Les règles administratives en matière de sécurité se présentent sous la forme de deux règles générales, suivies des règles relatives aux exigences DICAI en matière de sécurité, soit :

1. Règles générales :

- **Points d'accès au réseau informatique ministériel** (ADMSG01) : les points d'accès au réseau informatique ministériel sont déterminés, justifiés et rendus opérationnels en fonction de la stratégie d'affaires du Ministère et des impératifs opérationnels, et ce, seulement après avoir été formellement autorisés par les autorités compétentes;
- **Respect des normes et règles d'accès au réseau** (ADMSG02) : toutes les applications et tous les services technologiques sont élaborés selon des normes et des règles relatives à la sécurité informatique, en conformité avec les standards ayant cours dans l'appareil public.

2. Règles relatives à la disponibilité :

- **Relève et continuité des opérations-1** (ADMSD01) : les services réseau essentiels à l'organisation comportent un système de relève adéquat, dont le fonctionnement est vérifié régulièrement, en fonction des objectifs de l'organisation et des ententes convenues avec les clientèles et partenaires;
- **Relève et continuité des opérations-2** (ADMSD02) : des mécanismes appropriés assurent la surveillance régulière des composants du réseau informatique ministériel (antivirus, détection des intrusions, détection des anomalies...);
- **Offre de service du réseau informatique** (ADMSD03) : la disponibilité du réseau informatique ministériel et les mécanismes qui l'assurent reposent sur l'offre de service du Ministère, elle-même appuyée sur la stratégie d'affaires et les impératifs opérationnels du Ministère.

3 Et en particulier, d'un réseau de télécommunications d'envergure réparti sur l'ensemble du territoire québécois, aussi appelé le réseau informatique ministériel (RIM), comprenant le réseau étendu (WAN), les réseaux locaux (LAN), les serveurs ministériels et les serveurs locaux.

3. Règles relatives à l'intégrité :

- **Intégrité des sources et des données-1** (ADMSI01) : toutes les informations numériques qui entrent dans le réseau informatique ministériel doivent provenir de sources connues, identifiables et vérifiables, et doivent également être soumises à des mécanismes de vérification de leur intégrité;
- **Intégrité des sources et des données-2** (ADMSI02) : des évaluations régulières du fonctionnement des solutions mises en place en matière de sécurité informatique doivent être effectuées (vérifications et audits);
- **Gestion des événements de sécurité** (ADMSI03) : tous les incidents relatifs à la sécurité (exploitation et utilisation de l'infrastructure technologique ministérielle) doivent être consignés dans des registres exploitables, vérifiés à intervalles réguliers;
- **Intégrité des composants informatiques-1** (ADMSI04) : des mécanismes appropriés et vérifiables doivent assurer l'intégrité des composants informatiques (signature des composants, antivirus, détection des intrusions, anomalies...);
- **Intégrité des composants informatiques-2** (ADMSI05) : les équipements informatiques du Ministère (ex. : postes de travail) utilisés à distance par des employés doivent être protégés adéquatement lorsqu'ils sont directement raccordés à un réseau public ou à un réseau dont les caractéristiques sur le plan de la sécurité ne peuvent être certifiées par le Ministère;
- **Intégrité des composants informatiques-3** (ADMSI06) : le raccordement du réseau informatique ministériel à des réseaux externes ne peut s'appuyer sur des liens de confiance que si une entente officielle intervient entre les parties concernées.

4. Règles relatives à la confidentialité :

- **Transit des données numériques du Ministère** (ADMSC01) : toutes les informations numériques de nature personnelle ou confidentielle détenues par le Ministère qui transitent depuis le réseau informatique ministériel vers un point d'accès extérieur à ce réseau doivent obligatoirement être chiffrées;
- **Données numériques du Ministère conservées hors du réseau ministériel et des réseaux locaux** (ADMSC02) : les informations numériques de nature personnelle ou confidentielle conservées sur des postes de travail (ex. : postes portables) doivent faire l'objet de mesures de protection adéquates (isolation physique, chiffrement, pare-feu...);
- **Localisation des données nominatives et confidentielles** (ADMSC03) : les informations numériques de nature personnelle et confidentielle détenues par le Ministère doivent être conservées à l'intérieur de zones ou d'environnements protégés;
- **Contrôle sur la base de privilèges d'accès** (ADMSC04) : les privilèges d'accès aux infrastructures, services et informations personnelles ou confidentielles doivent correspondre aux tâches des

utilisateurs internes ou faire l'objet d'ententes avec les clientèles ou partenaires externes;

- **Utilisation du périmètre de sécurité du Ministère** (ADMSC05) : tous les accès entrants et sortants du réseau informatique ministériel doivent obligatoirement transiter par un « périmètre » dont le fonctionnement est rigoureusement contrôlé, vérifiable et sécurisé.

5. Règles relatives à l'authentification :

- **Authentification des utilisateurs-1** (ADMSA01) : l'accès à des informations numériques de nature personnelle ou confidentielle, à des infrastructures ou à des services informatiques pouvant y donner accès nécessite obligatoirement une authentification préalable des utilisateurs, internes ou externes;
- **Authentification des utilisateurs-2** (ADMSA02) : l'identification et l'authentification de tous les utilisateurs internes ou externes accédant au réseau informatique ministériel, lorsque requises, doivent être effectuées dès leur introduction dans le périmètre de sécurité du réseau, par les moyens appropriés;
- **Authentification des utilisateurs-3** (ADMSA03) : les accès sortants du réseau informatique ministériel sont réservés aux utilisateurs internes dont l'authentification a préalablement été effectuée.

6. Règle relative à l'irrévocabilité :

- **Journalisation des accès et des activités** (ADMSR01) : les accès au réseau informatique ministériel et l'utilisation des services ou des applications qui y sont disponibles doivent reposer sur des moyens et des processus permettant d'assurer la vérifiabilité des actions effectuées et des accès autorisés auprès de l'infrastructure technologique ministérielle.

7 Mesures relatives à l'application de la politique

7.1 Architecture de la sécurité de l'information numérique (ASIN)

L'Architecture de la sécurité de l'information numérique (ASIN) vise à présenter la structure et le fonctionnement de la sécurité de l'information numérique et des échanges électroniques au Ministère, dans le respect des dimensions juridique, humaine, organisationnelle et technologique, telles qu'elles sont définies dans l'AGSIN[4].

L'architecture doit, entre autres, couvrir les points suivants :

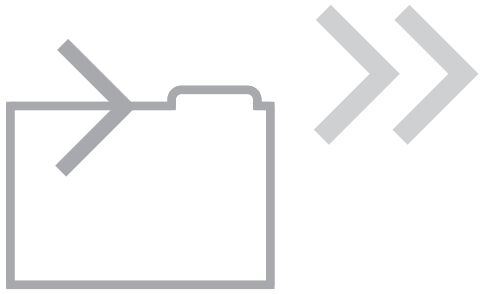
- la définition des principes et des orientations architecturales, en conformité avec la présente politique;
- la conception d'un modèle cible en matière de sécurité de l'information;
- la conception d'un modèle opérationnel, définissant les grandes fonctions qui sous-tendent la sécurité de l'information.

7.2 Cadre de gestion de la sécurité de l'information

Le cadre de gestion fait partie des mesures que le Ministère entend prendre pour mettre en application la présente politique. Ce cadre définit les rôles et les responsabilités en matière de gestion de la sécurité, notamment les mécanismes de coordination, de collaboration et de contrôle.

7.3 Registre d'autorité de la sécurité

Le cadre de gestion est concrétisé par un registre où sont consignés les noms des personnes qui sont affectées à des responsabilités particulières en ce qui a trait à la gestion de la sécurité de l'information. Ce registre constitue une mesure importante dans le cadre de l'application de la présente politique.



8 Directives découlant de la politique

Pour s'assurer que les lignes directrices régissant la sécurité de l'information soient connues, comprises et appliquées au sein de son organisation, le ministère des Transports entend élaborer les directives suivantes :

- Directive sur l'utilisation des technologies de communication sans fil;
- Directive sur le contrôle des accès.

4 L'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) est disponible sous une forme sommaire à http://www.autoroute.gouv.qc.ca/ publica/pdf/agsin-ciblesom.pdf

9 Rôles et responsabilités dans l'application de la politique

9.1 Le propriétaire des ressources informationnelles

Le propriétaire des ressources informationnelles est le sous-ministre. Il est le premier responsable de l'application de la présente politique. Ses principales responsabilités, en ce qui a trait à la sécurité, sont les suivantes :

- définir clairement les valeurs organisationnelles et les orientations internes, les faire partager par l'ensemble de son personnel et les communiquer à ses partenaires pour s'assurer qu'elles soient respectées;
- instaurer un mécanisme d'identification et d'évaluation périodique des risques et d'évaluation des mesures de sécurité en vigueur par rapport à ces derniers;
- établir un plan global de gestion de la sécurité, incluant les mesures de sécurité à mettre en œuvre, et le réviser périodiquement;
- assigner la responsabilité de toute information numérique ou toute technologie de l'information à un « détenteur », qui devra s'assurer, en collaboration avec le coordonnateur ministériel de la sécurité de l'information[5], que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement; le nom des détenteurs et leurs responsabilités devront être consignés dans le Registre d'autorité de la sécurité de l'information du ministère des Transports;
- inclure dans les ententes et les contrats des dispositions garantissant le respect des exigences en matière de sécurité définies par le Conseil du trésor;
- faire en sorte que le niveau de sécurité appliqué aux informations numériques qu'il reçoit ou communique à un autre ministère ou organisme ou à un tiers respecte les exigences prescrites par les lois, les règlements ou les directives;
- assurer la sensibilisation et la formation de son personnel en matière de sécurité;
- procéder à l'analyse systématique des incidents ayant mis ou qui auraient pu mettre en péril la sécurité;
- mettre en place des mécanismes d'évaluation et de contrôle assurant l'application efficace des orientations et des mesures adoptées en matière de sécurité, en impliquant notamment la Direction de la vérification interne et de l'évaluation de programmes ainsi que le Service des enquêtes;
- soumettre annuellement au Secrétariat du Conseil du trésor le bilan annuel, et aux instances désignées tout autre renseignement requis, conformément aux instructions gouvernementales;
- instaurer des mécanismes de coordination et de collaboration;
- collaborer aux travaux du réseau d'experts et de vigie lorsque le Secrétariat du Conseil du trésor le demande.

5 La directive gouvernementale sur la sécurité de l'information prévoit que le sous-ministre nomme un responsable de la sécurité de l'information numérique (RSIN) pour assurer la gestion et la coordination de la sécurité et le représenter en cette matière dans l'organisation. Celui-ci est désigné sous le nom de coordonnateur ministériel de la sécurité de l'information.

9.2 Le responsable de la protection des renseignements personnels (RPRP)

Le responsable ministériel de la protection des renseignements personnels, qui relève directement du sous-ministre :

- s'assure que la protection accordée par le Ministère aux renseignements qu'il détient répond aux normes légales, réglementaires, gouvernementales et ministérielles;
- agit comme répondant, tant au sein du Ministère qu'auprès des partenaires externes, en ce qui concerne la protection des renseignements détenus par le Ministère;
- coordonne le suivi des recommandations émises par les entités habilitées relativement à la protection des renseignements détenus par le Ministère, et ce, dans certains cas, avec la collaboration de la Direction de la vérification interne et de l'évaluation de programmes et le Service des enquêtes;
- coordonne les demandes de commentaires de la Commission d'accès à l'information à la suite de plaintes venant de la population;
- effectue le suivi des ententes sur les échanges d'informations;
- coordonne et supervise la tenue d'activités de sensibilisation à la protection des renseignements détenus par le Ministère;
- conseille le ministre, le sous-ministre et le personnel du Ministère en matière de protection des renseignements.

9.3 Le coordonnateur ministériel de la sécurité de l'information

En conformité avec la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale, le coordonnateur ministériel de la sécurité de l'information, désigné par le sous-ministre, est chargé d'assurer la gestion et la coordination de la sécurité et de le représenter en cette matière au sein du ministère des Transports. Ses principales responsabilités sont les suivantes :

- conseiller le sous-ministre dans la définition des orientations stratégiques et des priorités en matière de sécurité de l'information;
- participer aux mécanismes de coordination et de collaboration, et au besoin y représenter le sous-ministre;
- s'assurer de l'évaluation et de la gestion des risques pour la sécurité de l'information;
- concevoir, soumettre pour approbation et mettre en œuvre un plan global de gestion de la sécurité permettant de réduire les risques à un niveau jugé acceptable et l'évaluer;
- déterminer quels sont les risques résiduels que doit assumer le sous-ministre;
- s'assurer de la prise en compte des orientations et des exigences en matière de sécurité lors de la conception, de la réalisation ou de la modification des processus d'affaires, des systèmes d'information et des infrastructures technologiques et émettre des avis à l'intention des gestionnaires et des détenteurs concernés;
- élaborer et tenir à jour le Registre d'autorité de la sécurité.

9.4 La Direction de la planification et des stratégies de l'information

La Direction de la planification et des stratégies de l'information (DPSI) a notamment pour mission la planification et le suivi des activités touchant les ressources informationnelles, la coordination des grands projets et l'élaboration du cadre de gestion des ressources informationnelles ministérielles. Dans ce contexte, la DPSI planifie et conçoit les orientations ministérielles en matière de sécurité et définit l'Architecture de la sécurité de l'information numérique (ASIN), incluant la prestation électronique de services (PES) et les systèmes de transport intelligent (STI). Les principales responsabilités de cette direction en matière de sécurité de l'information sont les suivantes :

- s'assurer de la prise en compte des lignes directrices de la présente politique dans toutes les tâches et activités liées à sa mission;
- assumer, dans le cadre de la coordination des grands projets ministériels, la planification du déploiement des solutions technologiques prévues dans la présente politique;
- fournir à l'organisation, dans le contexte de sa mission, une expertise en matière de sécurité de l'information;
- participer à la sensibilisation du personnel à la sécurité de l'information.

9.5 La Direction des systèmes et des technologies de l'information

Dans le cadre de sa mission, la Direction des systèmes et des technologies de l'information (DSTI) doit fournir aux unités administratives tous les produits et services nécessaires en matière de ressources informationnelles et conseiller les autorités ministérielles quant à la gestion de ces ressources. Plus spécifiquement, la DSTI doit répondre aux engagements ministériels en matière de planification opérationnelle et de plans d'investissements, de gestion de la sécurité des données et des systèmes, d'administration du réseau ministériel et de continuité des opérations. Dans ce contexte, la DSTI planifie, fournit et maintient en état les moyens techniques de sécurité et s'assure que ces moyens répondent aux exigences en matière de sécurité pour l'information ministérielle. Les principales responsabilités de cette direction en ce qui a trait à la sécurité de l'information sont les suivantes :

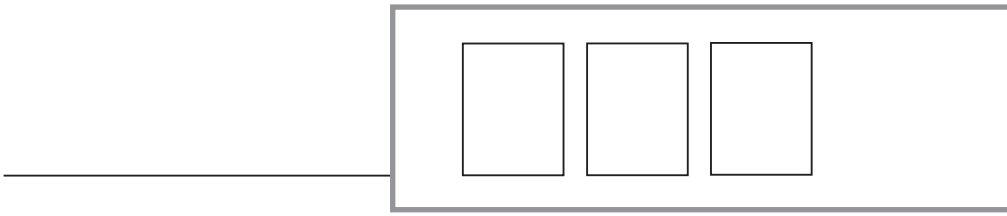
- s'assurer de la prise en compte des lignes directrices de la présente politique lors de l'acquisition ou de la conception, de la réalisation ou de la modification des systèmes d'information et des infrastructures technologiques;
- assurer la mise en œuvre de l'Architecture de la sécurité de l'information numérique (ASIN), conformément à la présente politique;
- élaborer les éléments normatifs découlant des lignes directrices de la présente politique;

- fournir à l'organisation une expertise en matière de sécurité de l'information numérique, notamment pour le développement de systèmes d'information;
- participer à la sensibilisation du personnel à la sécurité de l'information.

9.6 Le détenteur des ressources informationnelles (UA et UARS)

Le détenteur est le gestionnaire qui dirige une unité administrative (UA) ou une unité administrative responsable du système (UARS). Les détenteurs doivent s'assurer, en collaboration avec le coordonnateur ministériel de la sécurité de l'information, que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement. Les détenteurs sont désignés par le sous-ministre et leur nom est consigné au Registre d'autorité du Ministère. Ces détenteurs sont les premiers responsables de la gestion des ressources informationnelles, de leur utilisation et de l'application des mesures de contrôle nécessaires. Leurs principales responsabilités en ce qui a trait à la sécurité sont les suivantes :

- répondre de la sécurité des systèmes dont ils sont les détenteurs;
- définir les contours de leurs systèmes (traitement, ensemble de données, télécommunications, stockage, etc.);
- définir les risques relatifs à leurs systèmes;
- participer à la catégorisation de leurs systèmes en fonction de la valeur de l'information qu'ils contiennent et des risques qui les menacent;
- définir le niveau de protection actuel et le niveau visé;
- faire connaître leurs besoins en matière de sécurité au coordonnateur ministériel de la sécurité de l'information;
- voir à ce que les mesures de sécurité appropriées soient élaborées, mises en place et appliquées;
- définir les contrôles non informatiques (en aval et en amont de l'informatique);
- limiter le droit d'accès des utilisateurs aux seuls besoins liés à leur travail;
- s'assurer que les contrats ou les ententes de services signés avec les fournisseurs répondent aux critères de sécurité;
- participer à la mise au point du plan de sauvegarde et du plan de secours;
- superviser, conjointement avec le coordonnateur ministériel de la sécurité de l'information, les essais du plan de secours;
- contrôler la qualité des dispositifs de sécurité intégrés aux systèmes d'information lors de la conception, de la réalisation, de l'exploitation et de l'entretien;
- participer à la sensibilisation des utilisateurs aux exigences en matière de sécurité relatives à l'information qu'ils manipulent;
- contrôler la qualité des mesures de sécurité relevant de leur responsabilité.



9.7 Le gestionnaire

Les responsabilités du gestionnaire (incluant les gestionnaires des mandataires, partenaires et fournisseurs du Ministère) en ce qui a trait à la protection des ressources informationnelles sont, entre autres :

- d'informer et de sensibiliser son personnel sur les dispositions de la présente politique et les modalités liées à sa mise en œuvre;
- de s'assurer que les ressources de l'inforoute sont utilisées en conformité avec les principes directeurs de la présente politique;
- de répondre de l'utilisation qui est faite par son personnel des ressources informationnelles du Ministère;
- de répondre de l'utilisation qui est faite par le personnel et par les partenaires du Ministère des données dont il est le responsable. À cet égard, il doit voir à élaborer les protocoles d'entente avec les entités utilisatrices et à les faire respecter.

9.8 L'utilisateur

L'utilisateur (incluant les mandataires, partenaires et fournisseurs du Ministère) a l'obligation de protéger les ressources informationnelles mises à sa disposition, en les utilisant avec discernement et aux seules fins prévues. Les responsabilités de l'utilisateur en ce qui a trait à la protection des ressources informationnelles sont, entre autres :

- de prendre connaissance de la présente politique et de la respecter;
- d'utiliser les ressources informationnelles en se limitant aux fins pour lesquelles elles sont destinées et à l'intérieur des accès qui lui sont autorisés;
- de se conformer aux exigences légales dans l'utilisation des produits à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle et dans l'utilisation des produits logiciels propriétaires;
- de respecter les consignes et directives établies, conformément aux dispositions de la présente politique;
- de signaler sans tarder à son gestionnaire tout acte qui pourrait constituer une violation des orientations ministérielles en matière de sécurité de l'information.

10 Mesures disciplinaires

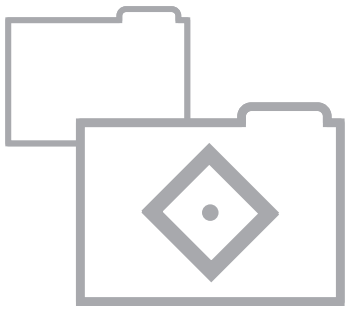
Lorsqu'un utilisateur contrevient à la présente politique ou aux directives internes qui en découlent, le sous-ministre détermine, selon la gravité du cas, s'il y a lieu d'appliquer une sanction disciplinaire ou une mesure administrative pouvant inclure une réprimande, une suspension ou un congédiement, et ce, conformément aux dispositions des conventions collectives ou des ententes. L'interdiction d'utiliser la ressource informationnelle en cause pourrait également être envisagée.

Le sous-ministre pourra aussi transmettre aux autorités judiciaires compétentes les informations qui l'incitent à croire qu'une infraction à une loi ou à un règlement en vigueur a été commise.

11 Entrée en vigueur et révision de la politique

La présente politique est actuellement en vigueur et remplace l'ancienne Politique de sécurité de l'information, adoptée en 1999.

Elle sera révisée sur une base triennale et chaque fois que des changements notables y seront apportés, afin de s'assurer qu'elle réponde bien aux besoins du ministère des Transports en matière de sécurité de l'information. Toute modification apportée à la présente politique doit être approuvée par le sous-ministre.



12 Définitions

Actif informationnel : une information, une banque d'information électronique, 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.

Cycle de vie de l'information : ensemble des étapes que franchit une information (électronique ou non) et qui vont du moment où le besoin d'informer se fait sentir et où cette information est structurée, jusqu'au moment où elle devient périmée, en passant par les différentes phases de son évolution et de sa diffusion.

Document technologique : document dont le support fait appel aux technologies de l'information, notamment celles qui sont mentionnées au second paragraphe de l'article 1 de la Loi concernant le cadre juridique des technologies de l'information : électronique, magnétique, optique, sans fil ou autres.

Fournisseur : entreprise, société, coopérative, personne physique ou tout fonds spécial du gouvernement qui fait affaires avec un ministère ou un organisme en vue de lui fournir des services ou des biens informatiques.

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

Logiciel propriétaire : se dit de tout produit informatique qui est propre à un constructeur ou un développeur donné, ce qui veut dire qu'il n'est pas nécessairement conforme à une norme ou un standard, qu'il n'est pas toujours compatible avec d'autres produits, qu'il est protégé par le droit d'auteur et qu'il faut l'acheter ou acquérir une licence pour pouvoir l'utiliser.

Plan de continuité : outil organisationnel et composante essentielle d'un plan de sécurité informatique, qui prévoit tous les cas possibles d'arrêt des ressources informatiques, de même que toutes les mesures applicables à chacun de ces cas, afin que soit assurée, sur site ou hors site, la continuité du service; il prévoit tous les cas, depuis l'incident mineur jusqu'au sinistre le plus grave.

Renseignement confidentiel : 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 sur la protection des renseignements personnels.

Renseignement nominatif : renseignement qui concerne une personne physique et qui permet de l'identifier.

Renseignement sensible : tout renseignement que le Ministère considère comme confidentiel, stratégique, essentiel, critique, indispensable ou vital pour ses opérations, et dont la divulgation, l'altération, la perte ou la destruction est susceptible de porter un préjudice au Ministère ou à sa clientèle, ses mandataires, partenaires et fournisseurs.

Ressources informationnelles : actifs informationnels et 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 : ensemble des moyens juridiques, humains, organisationnels et technologiques permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information. Ces moyens visent également une saine gestion des risques et de leurs effets quant à l'authentification des personnes et des dispositifs de même qu'à l'irrévocabilité des actions menées.

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

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

Annexe A - Références sur la sécurité de l'information

Titre et adresse du document

Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale

http://www.intranet.qc/hebergementdoc/directive/securite-informationnelle/securite.htm

Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique

http://www.rpg.tresor.qc/pdf/1-1-1-5.pdf

Déclaration de valeurs de l'administration publique québécoise

http://www.intranet.qc/hebergementdoc/ethique/declaration.pdf

Les règles en matière de sécurité de l'information numérique

http://www.intranet/dsti/abdf/securite_informatique3.pdf

La Directive 4.4.1 du Manuel administratif, volume IV, sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

http://www.intranet/BSM/secretariat/secretariat/4-4-01%20_2002-01_.pdf


Transports
Québec
confidentialité
disponibilité
intégrité
accès