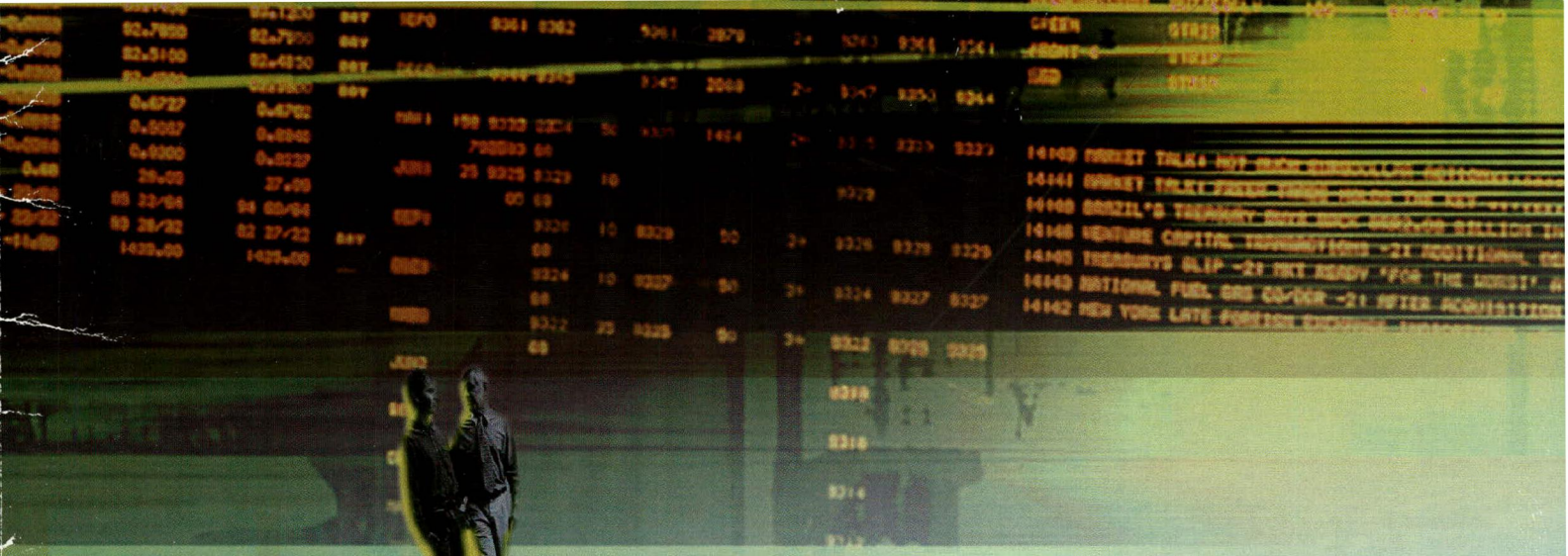


DIRECTIVE SUR LA SÉCURITÉ PHYSIQUE DES ACTIFS INFORMATIONNELS

Québec

DIRECTIVE
SUR LA SÉCURITÉ
PHYSIQUE DES ACTIFS
INFORMATIONNELS

Québec

La Directive sur la sécurité physique des actifs informationnels a été préparée par la Direction générale des services à la gestion et le Service des enquêtes du ministère des Transports du Québec. Elle a été éditée par la Direction des communications.

ISBN 2-550-45710-2
ISBN 2-550-45711-0 (PDF)
Dépôt légal
Bibliothèque nationale du Québec, 2005

Table des matières

1 Introduction 5

2 Secteur d'application 5

3 Modèle intégré des mesures de sécurité physique 6

4 Lignes directrices 7

5 Rôles et responsabilités 13

1 Introduction

Le ministère des Transports recueille, manipule, utilise et élimine, sous plusieurs formats et sur différents supports, de l'information nécessaire à la réalisation de sa mission. Le Ministère a établi, dans sa Politique de sécurité de l'information, que les ressources informationnelles, constituées des actifs informationnels et des ressources humaines, matérielles et financières qui leur sont associées sont essentielles à la réalisation de ses activités et qu'elles doivent faire l'objet d'une utilisation et d'une protection adéquates.

Or, l'information, indépendamment de son format et de sa structure, réside toujours sur un support physique tel qu'un ordinateur de bureau, un serveur de fichier ou de base de données du réseau, une disquette, un document papier, un microfilm ou autre. Incidemment, le support physique, quelle que soit sa nature ou sa forme, constitue un actif informationnel qui doit faire l'objet de mesures de sécurité adéquates afin de protéger l'information qu'il abrite. Même avec la meilleure sécurité informatique qui soit, la sécurité de l'information n'est complète que lorsque l'accès, l'utilisation et la manipulation des supports qui abritent l'information sont adéquatement contrôlés et que ces supports sont protégés contre les conditions environnementales et contre les risques d'accident, d'erreurs ou de malveillance auxquels ils sont exposés.

De la présente directive sur la sécurité physique des actifs informationnels découlera une série de mesures prévues aux diverses sections du modèle intégré décrit à la partie 3, et ce afin d'atteindre les objectifs ministériels de sécurité de l'information. Elle s'inscrit dans le plan global de gestion de la sécurité et s'ajoute aux directives découlant de la Politique de sécurité de l'information. La sécurité physique des actifs informationnels s'avère donc fondamentale pour le ministère des Transports et elle constitue une priorité majeure.

Après avoir déterminé la valeur de ses actifs-clés à l'aide du *Guide de catégorisation des actifs informationnels* du ministère des Transports, chaque unité administrative pourra appliquer la présente directive aux actifs catégorisés. Pour atteindre les objectifs énoncés et dans le but d'assurer une gestion adéquate et cohérente des mesures de sécurité physique des actifs informationnels de l'ensemble du Ministère, la directive présente :

- une définition du secteur d'application de la sécurité physique des actifs informationnels;
- un modèle intégré des mesures de sécurité physique;
- des lignes directrices qui précisent les préoccupations de sécurité physique des actifs informationnels et qui constituent l'assise des normes, règles et procédures à respecter en cette matière;
- une définition des rôles et responsabilités nécessaires pour garantir l'atteinte des objectifs en matière de sécurité physique des actifs informationnels du Ministère.

2 Secteur d'application

La directive ministérielle sur la sécurité physique des actifs informationnels porte sur les actifs informationnels physiques détenus ou utilisés par l'ensemble des unités administratives du Ministère, et ce, tout au long de leur cycle de vie et sans égard à leur localisation. Les actifs informationnels physiques incluent l'ensemble des supports qui abritent, traitent ou transforment de l'information nécessaire pour la réalisation des activités du Ministère, dont :

- les supports de stockage de l'information (communément appelés « documents ») sous toutes leurs formes - papier, microfilms et supports électroniques, magnétiques, optiques ou autres ou faisant appel à une combinaison de technologies;

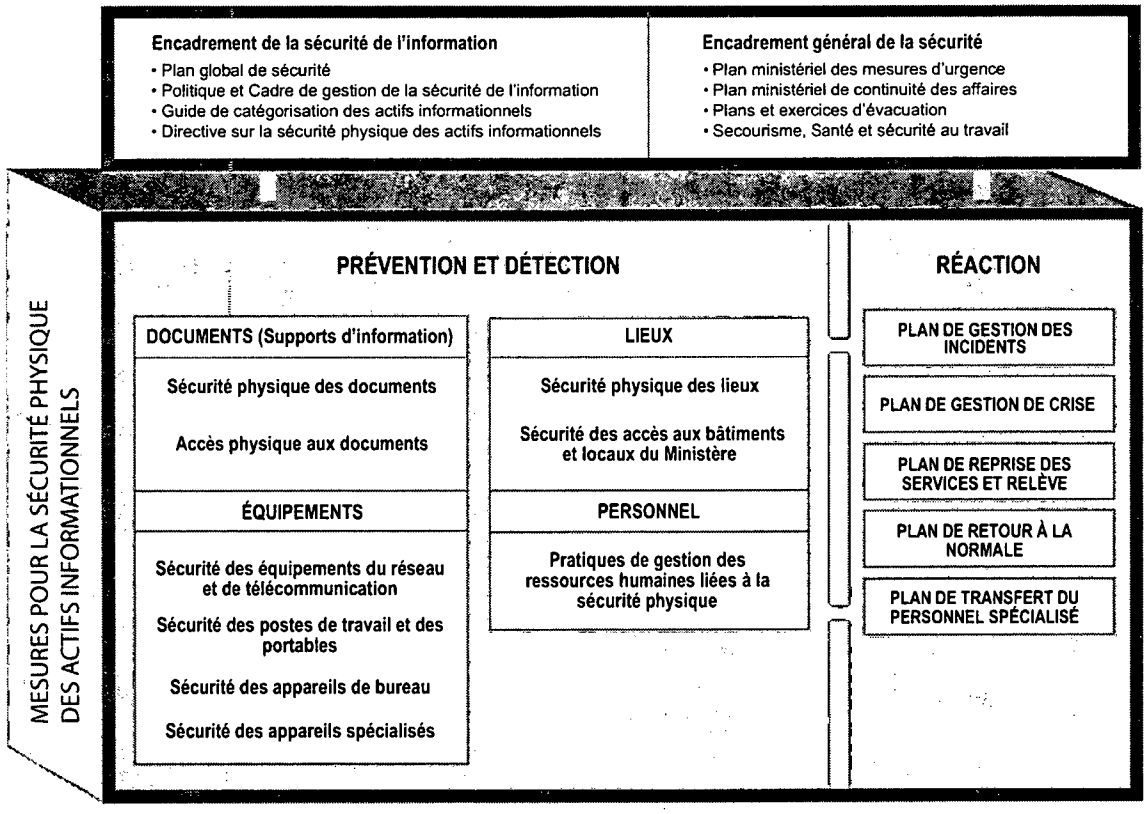
- les équipements informatiques mis à la disposition du personnel - postes de travail, micro-ordinateurs portatifs et assistants numériques personnels;
- les équipements du réseau et de télécommunication - commutateurs, routeurs, modems, serveurs, câblage, etc.;
- les appareils de bureau - imprimantes, photocopieurs, télécopieurs, etc.;
- les appareils spécialisés de collecte d'information utilisés par le Ministère - caméras de surveillance du réseau routier, appareils à l'intérieur de véhicules pour la collecte de données sur l'état du réseau routier, etc.

La présente directive s'applique à toute personne qui manipule ou utilise les actifs informationnels du Ministère, et ce, sans égard au statut d'emploi - personnel régulier, occasionnel ou contractuel. Les partenaires, mandataires et fournisseurs sont soumis aux mêmes obligations que le personnel lorsqu'ils manipulent ou utilisent les actifs informationnels du Ministère.

3 Modèle intégré des mesures de sécurité physique

Afin de dégager une vision globale des mesures de sécurité physique à mettre en place pour protéger ses actifs informationnels, le ministère des Transports s'est doté d'un modèle intégré des mesures de sécurité physique. Ce modèle permet de structurer les mesures de sécurité physique des actifs informationnels et illustre les liens avec l'encadrement de la sécurité de l'information et l'encadrement général de la sécurité au Ministère.

Modèle intégré des mesures de sécurité physique



Tel qu'il est illustré, les mesures de sécurité physique sont structurées en deux grands blocs qui sont les mesures de *prévention* et *détection* et les mesures de *réaction.*

Les mesures de *prévention et détection* regroupent les mesures de sécurité applicables aux actifs informationnels physiques du Ministère qui sont les supports de stockage de l'information, communément appelés « documents », les équipements informatiques personnels, les équipements du réseau et de télécommunication, les appareils de bureau et les appareils spécialisés de collecte d'information. À ces mesures s'ajoutent les mesures de sécurité physique des lieux qui abritent les actifs informationnels ainsi que les mesures visant à sensibiliser et à former le personnel du Ministère à la sécurité physique des actifs informationnels.

Les mesures de *réaction* concernent les mesures de sécurité physique qui doivent être intégrées dans les différents plans exécutés à la suite d'un incident ou d'un sinistre. Ces différentes mesures permettent de réduire les impacts pour le Ministère lorsque ses actifs informationnels physiques ont été affectés par un incident ou un sinistre.

4 Lignes directrices

Pour atteindre ses objectifs de sécurité de l'information, le ministère des Transports énonce les lignes directrices qui suivent en matière de sécurité physique des actifs informationnels.

4.1 Énoncés généraux

Les mesures de sécurité physique des actifs informationnels couvrent tout le cycle de vie des actifs informationnels à protéger, depuis leur acquisition ou leur création jusqu'à leur élimination.

Les mesures de sécurité physique des actifs informationnels s'harmonisent avec les mesures de sécurité plus générales du Ministère telles que la sécurité du milieu et des biens, la sécurité du personnel, les mesures d'urgence et la continuité des affaires.

Les mesures de sécurité physique des actifs informationnels sont définies en fonction des critères de disponibilité, d'intégrité, de confidentialité, d'authentification et d'irrévocabilité des informations que ces actifs abritent, traitent ou transforment, des risques qui les menacent et de leur valeur.

Les mesures de sécurité physique des actifs informationnels couvrent la prévention, la détection et la réaction :

- les mesures de prévention concernent tous les moyens nécessaires pour protéger les actifs informationnels contre les risques de dysfonctionnement (ex. : bris causé par l'usure ou par un manque d'entretien), contre les actes malveillants ou non intentionnels - compromission, vol ou vandalisme, connexions non autorisées, etc. - ainsi que contre les menaces attribuables à l'environnement : poussière, humidité, chaleur, etc.;
- les mesures de détection couvrent tous les moyens nécessaires pour détecter un événement ou un incident qui porte, ou pourrait porter, atteinte à la sécurité physique des actifs informationnels du Ministère;
- les mesures de réaction, appliquées à la suite d'un incident ou d'un sinistre, concernent tous les moyens permettant de limiter les impacts d'un incident ou d'un sinistre sur les actifs informationnels et sur le Ministère.

4.2 Sécurité physique des documents

Les documents à protéger sur support physique - papier, audio, vidéo, microfilm, etc. - et sur des supports de stockage numériques utilisés par le personnel du Ministère - disques, disquettes, unités de stockage USB, etc. - font l'objet de mesures de sécurité physique.

Il est entendu, par « document à protéger », l'ensemble des documents qui doivent faire l'objet de mesures de sécurité physique particulières, tels que les documents contenant des informations nominatives ou confidentielles, les documents stratégiques, les documents essentiels pour la continuité des affaires, les documents à valeur patrimoniale, les documents recueillis ou conservés aux fins de preuve ou tout autre document d'une valeur particulière pour le Ministère et déterminé par un exercice de catégorisation[1].

Les mesures de sécurité physique des documents à protéger doivent notamment couvrir :

- l'accès physique aux documents. L'accès physique aux documents à protéger est limité par des mesures de sécurité physique appropriées (ex. : classeur à haute sécurité) et doit être explicitement autorisé et contrôlé (ex. : journalisation des consultations);
- le transport, la transmission ou l'expédition des documents - en personne, par messagerie, par courrier interne, par la poste ou par tout autre mode de transmission. Ces mesures incluent la prise en considération des risques liés à la perte, à une mauvaise manipulation ou au vol des documents, et ce, notamment pour les copies de sauvegarde transportées à l'extérieur du Ministère;
- l'utilisation des documents à l'extérieur du Ministère. En règle générale, les documents, qu'ils soient sur des supports physiques ou sur des supports de stockage numériques, doivent demeurer sur les lieux de travail. Quiconque est autorisé à transporter ou à travailler avec des documents à l'extérieur du périmètre des lieux de travail du Ministère (ex. : dans le contexte du télétravail) doit prendre les mesures de sécurité physique nécessaires pour assurer leur protection;
- la numérisation, le transfert de support et la prise de copies de documents de façon sécuritaire;
- la conservation des documents à protéger dans des contenants et des lieux sécuritaires;
- la constitution d'un plan de sauvegarde et de récupération des documents à protéger précisant, entre autres, la fréquence des copies de sécurité, le lieu d'entreposage de ces copies, les personnes responsables de cette activité et les calendriers de conservation :
  - les copies de sauvegarde, particulièrement celles contenant des documents essentiels pour la continuité des affaires, sont entreposées dans des contenants sécuritaires et à l'extérieur de leur lieu d'origine;
  - la circulation des copies de sauvegarde est contrôlée et l'accès à celles-ci est restreint aux seules personnes autorisées;
  - les procédures de sauvegarde et de récupération sont définies par écrit et tenues à jour;
  - les copies de sauvegarde et les mécanismes de récupération des informations qu'elles contiennent sont vérifiés régulièrement;

1. La catégorisation des actifs informationnels est réalisée à l'aide du Guide de catégorisation des actifs informationnels du ministère des Transports. Pour la procédure de gestion des documents papier actifs, il faut se référer à la directive 4-3-4 (Volume IV) du *Manuel administratif* du ministère des Transports.

- l'élimination et la destruction de façon sécuritaire. La mise au rebut ou le recyclage des documents contenant des renseignements nominatifs ou de nature sensible doit être effectué selon les règles en vigueur, de telle sorte que leur caractère confidentiel soit protégé et que la reconstruction des données antérieures soit impossible. Les supports de stockage numériques doivent notamment être effacés avant que ceux-ci soient mis au rebut, réutilisés à d'autres fins ou récupérés par un fournisseur;
- l'archivage selon le calendrier de conservation.

4.3 Sécurité des équipements (énoncés généraux)

Des mesures de sécurité physique sont appliquées aux équipements et infrastructures de traitement de l'information du Ministère. Les mesures générales doivent notamment prévoir :

- un inventaire des équipements, précisant leur localisation et leur assignation principale;
- un calendrier des tâches d'installation et un registre de l'entretien des équipements, selon les normes des fournisseurs ou des fabricants;
- la protection des équipements contre l'utilisation non autorisée et le vol;
- le contrôle et le suivi des équipements transportés ou utilisés hors des installations du Ministère;
- l'élimination de l'information contenue sur tout équipement déclaré en surplus ou mis au rebut.

4.3.1 Sécurité des équipements du réseau et de télécommunication

Des mesures de sécurité physique sont appliquées pour protéger les équipements du réseau et de télécommunication du Ministère qui abritent, traitent ou transforment de l'information. Il est entendu, par « équipements du réseau et de télécommunication », l'ensemble des équipements utilisés pour le traitement de l'information numérique, tels que les concentrateurs, les commutateurs, les routeurs, les modems, le matériel de surveillance et d'administration, les serveurs, les équipements de télécommunication, le câblage, les dispositifs d'alimentation, les unités de climatisation, etc.

Les mesures de sécurité physique des équipements du réseau et de télécommunication doivent notamment prévoir :

- la localisation des équipements dans des emplacements exclusivement réservés à leur hébergement;
- la protection des équipements contre les risques de dysfonctionnement attribuables à la poussière, à la température, à l'humidité relative de l'air, aux vibrations, aux erreurs de manipulation ou d'entretien, à l'électricité statique, aux surtensions, aux interférences et au brouillage de signal;
- la protection contre la connexion ou le branchement d'appareils non autorisés - écoute, récupération, modification d'informations;
- la protection contre toute autre menace humaine, matérielle ou environnementale qui pourrait porter atteinte à la sécurité de l'information du Ministère.

Des solutions et des équipements de secours pour parer aux incidents ou aux sinistres affectant les équipements du réseau et de télécommunication sont également prévus. Ces solutions sont intégrées au plan de gestion des incidents et aux plans de reprise sur sinistre et de retour à la normale.

4.3.2 Sécurité des postes de travail et des portables

Des mesures de sécurité physique sont appliquées à l'ensemble des postes de travail et des portables qui abritent des documents du Ministère à protéger, tels que les ordinateurs de table, les micro-ordinateurs portatifs, les assistants numériques personnels et tout autre équipement micro-informatique, et ce, qu'ils soient situés dans ses locaux ou à l'extérieur de ses locaux (ex. : télétravail).

Ces équipements sont notamment protégés contre le vol ou l'utilisation non autorisée (ex. : burinage, câble antivol, conservation des clés, rangement de l'équipement dans du mobilier verrouillé, etc.), surtout lorsque ces équipements sont utilisés ou transportés à l'extérieur du périmètre des locaux du Ministère.

4.3.3 Sécurité des appareils de bureau

Dans le cas où la confidentialité de l'information est une source de préoccupation, les appareils de bureau, tels que les imprimantes, les photocopieurs et les télécopieurs, doivent être positionnés dans des endroits contrôlés ou équipés de dispositifs de protection physique appropriés (ex. : recouvrements d'imprimante), de façon que l'information affichée ou traitée ne puisse être visualisée ou être facilement accessible à des personnes non autorisées.

4.3.4 Sécurité des appareils spécialisés

Les appareils spécialisés de collecte d'information utilisés par le Ministère, tels que les enregistreurs analogiques ou numériques reliés aux caméras de surveillance du réseau routier et les appareils à l'intérieur de véhicules pour la collecte de données sur l'état du réseau routier, font l'objet de mesures de sécurité physique appropriées selon la nature des informations qu'ils abritent ou traitent et leur degré d'exposition aux conditions environnementales.

4.4 Sécurité des lieux (énoncé général)

Des mesures de sécurité physique sont appliquées aux locaux et bâtiments qui abritent des actifs informationnels du Ministère. Ces mesures sont fonction de la nature des actifs qu'ils abritent - précisée par l'exercice de catégorisation - et prennent en considération les mesures générales de sécurité des lieux telles que leur conformité aux normes du bâtiment, les plans et exercices d'évacuation, les mesures d'urgence, la santé et la sécurité au travail et l'ergonomie.

4.4.1 Sécurité physique des lieux

Les mesures de sécurité physique des lieux doivent notamment prévoir :

- la mise en place de moyens de protection contre des catastrophes naturelles ou accidentelles - verglas, bris d'aqueduc, surchauffe, déclenchement de gicleurs, etc.;
- des mesures d'alimentation électrique sans interruption et des systèmes de protection contre les incendies;
- l'installation et l'entretien des systèmes de chauffage, de ventilation et de climatisation, et ce, conformément aux normes recommandées;
- les outils automatisés de détection d'incidents et en temps réel - feu, humidité élevée, panne d'électricité, etc. - avec un retour d'alarme vers un poste permanent et des fonctions de journalisation des événements de sécurité.

4.4.2 Sécurité des accès aux bâtiments et locaux du Ministère

Les mesures de sécurité des accès aux bâtiments et locaux du Ministère doivent notamment prévoir :

- la création de périmètres de sécurité clairement définis répondant aux exigences du Ministère, notamment dans les situations où les locaux sont partagés avec d'autres organisations;
- une liste des personnes autorisées à accéder aux bâtiments et aux locaux du Ministère;
- le contrôle des accès à l'entrée des bâtiments (ex. : postes de garde, cartes d'accès) et à l'entrée des locaux qui abritent les actifs informationnels à protéger;
- les mesures de protection contre le vol, le bris et la pénétration non autorisée - par les portes, fenêtres, conduits, sous-sol, etc.;
- la surveillance physique (ex. : patrouille et vérification par les gardiens) des lieux qui abritent des équipements et infrastructures de traitement de l'information considérés comme stratégiques pour le Ministère (ex. : centres de traitement informatique);
- les outils automatisés de détection d'incidents et en temps réel - portes laissées ouvertes, intrusions, etc. - avec un retour d'alarme vers un poste permanent et des fonctions de journalisation des événements de sécurité;
- les systèmes de surveillance par caméra.

4.5 Pratiques de gestion des ressources humaines liées à la sécurité physique

Les préoccupations de sécurité physique des actifs informationnels sont intégrées aux pratiques du Ministère en matière de gestion des ressources humaines :

- les nouveaux employés sont informés de leurs responsabilités à l'égard de la sécurité physique des actifs informationnels;
- la sécurité physique des actifs informationnels est intégrée au programme ministériel de sensibilisation à la sécurité;
- une formation portant sur la sécurité physique est offerte à toutes les personnes assumant des responsabilités importantes en la matière;
- des vérifications périodiques sont effectuées afin de s'assurer que le personnel respecte les consignes de sécurité physique.

4.6 Mesures de réaction

Suivant le modèle intégré des mesures de sécurité physique, des mesures sont intégrées dans les différents plans exécutés à la suite d'un incident ou d'un sinistre, afin de minimiser les impacts pour le Ministère lorsque ses actifs informationnels sont affectés.

4.6.1 Plan de gestion des incidents

Le plan ministériel de gestion des incidents de sécurité doit inclure toutes les mesures à appliquer en réaction à un incident où la sécurité physique des actifs informationnels est en cause. Ce plan doit notamment couvrir :

- les modalités de signalement d'un incident de sécurité physique, les modalités d'escalade, l'analyse de l'incident, la réaction à l'incident, un plan de communication - incluant les forces de l'ordre - ainsi que le rétablissement de la situation à la suite de l'incident;

- les actions permettant la reconstitution des événements;
- les conditions de recommandation de lancement du plan de gestion de crise en cas d'insuccès des mesures énoncées dans le plan de gestion des incidents.

Signalement des incidents

- Tous les incidents ou actions portant ou pouvant porter atteinte à la sécurité physique des actifs informationnels doivent être rapportés aussitôt que possible. Le mécanisme de signalement des incidents existe et est connu du personnel.

Réaction à l'incident

- Un suivi des incidents de sécurité physique affectant les actifs informationnels est effectué. On note comment les incidents ont été traités, le déroulement des faits au cours de l'incident, le moment où l'incident a été détecté, les mesures prises, la logique à l'appui des décisions, le détail des communications, les autorisations de la direction ou ses consignes et les rapports externes et internes.

Analyse postérieure à l'incident

- Chaque fois que se produit un incident de sécurité physique grave ou majeur, une analyse postérieure à l'incident permet de résumer les effets de l'incident et d'énoncer :
  - les lacunes au chapitre de la sécurité physique des actifs informationnels,
  - les mesures qui empêcheront ce type d'incident de se reproduire,
  - les mesures permettant de réduire la possibilité d'une récurrence,
  - les améliorations à apporter aux procédures de traitement des incidents.

4.6.2 Plan de gestion de crise

Le plan de gestion de crise du Ministère, appliqué en cas d'insuccès des mesures mises en place dans le contexte du plan de gestion des incidents, doit prévoir les modalités selon lesquelles le comité de crise intervient à la suite d'un sinistre où la sécurité physique des actifs informationnels est gravement menacée.

4.6.3 Plan de reprise des services d'affaires

Le plan de reprise des services d'affaires, appliqué afin de rétablir les fonctions essentielles dans les limites de temps et selon les exigences de disponibilité précisées dans le Plan de continuité des services d'affaires du Ministère, doit notamment prévoir toutes les mesures de sécurité physique nécessaires pour l'atteinte des objectifs de reprise et pour assurer la protection des actifs informationnels du Ministère pendant la période de retour à la normale. Ce plan doit notamment prévoir :

- la prise de copies de sauvegarde pour la reprise et leur entreposage dans des contenants et des lieux sécurisés à l'extérieur du site;
- la mise à jour des documents relatifs au plan de reprise et leur conservation à l'extérieur du site;
- la détermination des mesures de sécurité physique applicables en situation de crise afin de protéger les actifs informationnels du Ministère;
- la mise à l'essai simultanée des mesures de sécurité physique et des mesures de sécurité logiques - plan de test incluant à la fois les mesures physiques et logiques - pour s'assurer qu'elles sont efficaces et qu'elles peuvent être appliquées dans les délais impartis;
- l'établissement des délais de conservation pour les données essentielles sur les activités et les copies de sauvegarde archivées;

- la consignation, dans un protocole d'entente ou toute autre convention, de tous les arrangements pris pour la sauvegarde à l'extérieur des installations du Ministère - dans les cas où la sauvegarde externe est sous le contrôle d'une tierce partie.

4.6.4 Plan de retour à la normale des services d'affaires

Le plan de retour à la normale des services d'affaires du Ministère, appliqué afin de permettre le retour à un site permanent - site d'origine ou de remplacement - après une situation de reprise hors site, doit prévoir toutes les mesures de sécurité physique nécessaires pour assurer la protection des actifs informationnels du Ministère pendant la période transitoire de retour à la normale.

4.6.5 Plan de transfert du personnel spécialisé

Le plan de transfert temporaire du personnel spécialisé, nécessaire en situation de reprise, doit notamment inclure le personnel assumant des responsabilités importantes en matière de sécurité physique des actifs informationnels.

5 Rôles et responsabilités

Cette section présente une définition des rôles et responsabilités nécessaires pour garantir l'atteinte des objectifs du ministère des Transports en matière de sécurité physique des actifs informationnels. Elle vient compléter l'annexe B du *Cadre de gestion de la sécurité de l'information* au ministère des Transports.

Il importe de rappeler que le sous-ministre est le seul propriétaire des actifs informationnels du Ministère et que les rôles suivants s'inscrivent dans le contexte particulier de l'application de la présente directive.

Le comité de gestion du Ministère

Le comité de gestion du Ministère a les responsabilités suivantes :

- approuver la Directive sur la sécurité physique des actifs informationnels;
- soutenir le sous-ministre dans la définition des valeurs organisationnelles et l'application des orientations internes du Ministère à l'égard de la sécurité physique des actifs informationnels.

Le Comité ministériel permanent de la sécurité de l'information (CSI)

Les responsabilités du CSI sont les suivantes :

- mandater des comités de travail ou des groupes spécifiques en matière de sécurité physique des actifs informationnels;
- tenir lieu de comité directeur en matière de sécurité physique des actifs informationnels pour les projets touchant l'ensemble du ministère des Transports;
- donner des avis et proposer au sous-ministre des orientations stratégiques en matière de sécurité physique des actifs informationnels.

Le responsable ministériel de la sécurité (RMS)

Les responsabilités du RMS sont les suivantes :

- assurer l'évolution de la présente directive;
- assurer la cohérence d'action nécessaire entre les exigences en matière de sécurité physique des actifs informationnels et les exigences plus générales de sécurité, telles que la sécurité du milieu et des biens, la sécurité du personnel, les mesures d'urgence et la continuité des affaires du Ministère;
- s'assurer, en collaboration avec les détenteurs, de la prise en considération des exigences de sécurité physique des actifs informationnels dans le contexte de la gestion de projets, de même que durant tout le cycle de vie des actifs informationnels à protéger;

- enclencher le Plan de reprise ministériel à la suite d'un sinistre majeur où la sécurité physique des actifs informationnels est en cause.

Le coordonnateur ministériel responsable de la sécurité de l'information numérique (RSIN)

Les responsabilités du RSIN sont les suivantes :

- s'assurer de la détermination et de la gestion contrôlée des risques d'atteinte à la sécurité physique des actifs informationnels du Ministère;
- s'assurer de la prise en considération des orientations et exigences en matière de sécurité physique des actifs informationnels lors de la conception, de la réalisation ou de la modification des processus d'affaires et des infrastructures technologiques et donner un avis de pertinence aux gestionnaires et aux détenteurs concernés;
- collaborer avec le RMS et le responsable de la sécurité physique à la détermination des priorités d'intervention en matière de sécurité physique des actifs informationnels;
- veiller à la prise en considération des préoccupations de sécurité physique dans tous les mécanismes de coordination et de collaboration - tables de coordination tactique de la sécurité, comité ministériel de PRP, etc.;
- s'assurer de la détermination et de la gestion des risques d'atteinte à la sécurité physique des actifs informationnels et, notamment, évaluer la vulnérabilité du ministère des Transports relativement à ceux-ci;
- coordonner la réalisation des activités de sensibilisation du personnel et de formation des spécialistes en matière de sécurité physique des actifs informationnels.

Le responsable de la sécurité physique (RSP)

Le responsable de la sécurité physique des actifs informationnels assume les rôles suivants :

- assurer, pour l'ensemble du ministère des Transports, la cohérence et la vision nécessaires à l'égard des mesures de sécurité physique des actifs informationnels;
- coordonner les travaux ministériels en matière de sécurité physique des actifs informationnels afin d'assurer l'arrimage entre les différents aspects de la sécurité physique et entre les divers intervenants assumant des responsabilités à cet égard;
- agir à titre d'expert-conseil en matière de sécurité physique des actifs informationnels dans les mécanismes de coordination et de collaboration : CSI, comité ministériel de PRP, tables de coordination tactique de la sécurité, etc.;
- soutenir le RSIN dans les domaines touchant la sécurité physique des actifs informationnels du Ministère;
- collaborer à la préparation du bilan annuel de sécurité du Ministère dans les domaines touchant la sécurité physique des actifs informationnels;
- déterminer et évaluer les risques, au regard de la sécurité physique, qui menacent la protection des actifs informationnels du Ministère;
- évaluer les mesures de sécurité physique et de contrôle à mettre en place pour assurer la protection des actifs informationnels du Ministère;
- veiller à la mise en application et procéder à des inspections et à des analyses relatives à la conformité d'application des mesures de sécurité physique des actifs informationnels et formuler les recommandations visant à assurer leur mise en place ainsi que leur suivi;
- soutenir le Service des enquêtes dans l'analyse et la prise en charge des incidents où la sécurité physique des actifs informationnels est en cause.

Le répondant local de la sécurité de l'information (RLSI)

Les responsabilités du RLSI sont les suivantes :

- assurer dans sa direction, en conformité avec les exigences du Ministère, une gestion efficace des mesures de sécurité physique des actifs informationnels et contrôler leur application;
- prendre en considération les exigences de sécurité physique des actifs informationnels lors des participations aux tables de coordination tactique de la sécurité;
- recueillir les besoins de sécurité physique des actifs informationnels auprès des détenteurs, notamment les besoins pour la reprise et les communiquer au RSP;
- produire, le cas échéant, les états de situation de la sécurité physique des actifs informationnels de sa direction;
- gérer la reprise des opérations, en direction territoriale, advenant un sinistre majeur.

Les tables de coordination tactique de la sécurité

Les tables de coordination tactique de la sécurité sont principalement composées des RLSI et des gestionnaires. Les responsabilités de ces tables sont les suivantes :

- donner des avis et proposer des orientations tactiques en matière de sécurité physique des actifs informationnels;
- communiquer les exigences du Ministère en matière de sécurité physique des actifs informationnels;
- rendre compte au RSIN et au RSP de l'application des mesures de sécurité physique des actifs informationnels.

Les détenteurs

Les détenteurs d'actifs sont les unités administratives (UA) et les unités administratives responsables de systèmes ministériels (UARS).

Outre les responsabilités attribuées aux détenteurs (UA et UARS) dans le contexte de la gestion de la sécurité de l'information, les détenteurs doivent s'assurer, en collaboration avec le RSIN, le RSP et les RLSI, que les mesures appropriées pour la sécurité physique des actifs informationnels sont élaborées, approuvées, mises en place et appliquées systématiquement.

Les responsabilités des détenteurs sont les suivantes :

- s'assurer que les exigences en matière de sécurité physique des actifs informationnels sont appliquées dès la conception, la réalisation ou la modification des processus d'affaires et des infrastructures technologiques;
- établir et maintenir à jour l'inventaire des actifs informationnels dont ils sont les détenteurs;
- catégoriser les actifs informationnels dont ils sont les détenteurs et déterminer les mesures de sécurité physique appropriées en fonction de la nature des informations incluses dans ces actifs et des risques qui les menacent;
- mettre au point un plan de sauvegarde ainsi qu'un plan de reprise dans le cadre du plan ministériel de continuité des affaires pour les actifs informationnels dont ils sont les détenteurs;
- pour les UARS, collaborer avec la DSTI à l'élaboration et aux tests du Plan de reprise ministériel, ainsi qu'à sa réalisation effective.

Le gestionnaire

Le gestionnaire doit s'assurer que la sécurité physique des actifs informationnels est prise en considération par le personnel de son unité administrative. Les responsabilités du gestionnaire sont les suivantes :

- s'assurer de mettre en place toute les mesures de sécurité physique nécessaires pour protéger les actifs informationnels de son unité administrative, et ce, notamment lors de la conception, de la réalisation ou de la modification des processus d'affaires et des infrastructures technologiques propres à son unité administrative;
- communiquer à l'ensemble de son personnel les exigences de protection en matière de sécurité physique des actifs informationnels et s'assurer qu'elles sont respectées;
- intégrer aux ententes et aux contrats qu'il entérine avec les fournisseurs, partenaires et mandataires des dispositions garantissant le respect des exigences en matière de sécurité physique des actifs informationnels et s'assurer qu'elles sont respectées;
- s'assurer que les accès aux actifs informationnels qu'il autorise sont conformes aux exigences du Ministère en matière de sécurité physique des actifs informationnels et aux règles établies par les détenteurs;
- aviser le répondant local des accès physiques (RLAP) des mouvements de personnel dans son unité administrative - par exemple, entrée en fonction d'un employé, changement d'unité administrative, absence prolongée et départ - pour octroyer ou retirer les droits d'accès aux locaux;
- informer le CMI et le Service des enquêtes de tout événement ayant mis ou qui aurait pu mettre en péril la sécurité physique des actifs informationnels du Ministère et, le cas échéant, participer à toute analyse qui pourrait être requise;
- contribuer à l'exercice annuel du bilan ministériel, ou au besoin, produire les états de situation sur la sécurité physique des actifs informationnels dans son unité administrative exigés par les autorités du Ministère.

Les informaticiens de la sécurité locale (STMU)

Les responsabilités des STMU sont les suivantes :

- participer à l'implantation et maîtriser les mesures de sécurité physique pour les systèmes et les réseaux, telles qu'entérinées ou définies par les détenteurs et les gestionnaires;
- planifier et coordonner la mise en œuvre du plan de reprise des fichiers de données et des systèmes locaux et s'assurer, en collaboration avec le RLSI, de l'intégration et de la prise en considération des mesures de sécurité physique dans les tests et les essais de reprise;
- réaliser la prise des copies de sécurité des serveurs ainsi que l'entreposage et la gestion sécuritaires des supports informatiques pour la reprise des données et des systèmes locaux;
- à l'égard de la gestion de la sécurité, soutenir les utilisateurs et, notamment, les détenteurs et les gestionnaires dans leurs efforts pour assurer les responsabilités qui leur sont attribuées.

Le répondant local des accès physiques (RLAP)

Il y a un répondant local des accès physiques pour chacun des édifices occupés par le Ministère. Les responsabilités du RLAP sont les suivantes :

- assurer la mise en œuvre et l'exploitation quotidienne du Système de contrôle des accès physiques et de gestion des alarmes des locaux occupés par le Ministère;
- à la requête des gestionnaires, accorder ou retirer le privilège d'accès aux locaux de l'édifice au personnel sous la responsabilité de ce gestionnaire et aux autres personnes accréditées par le Ministère;
- maintenir un registre des privilèges d'accès accordés ou retirés et en rendre compte périodiquement, ou au besoin, au RSP, au RLSI et aux gestionnaires du personnel ayant accès aux locaux de l'édifice.

Les équipes de réalisation et les pilotes

Les principales responsabilités des équipes de réalisation - chefs de projets, analystes, développeurs - et des pilotes à l'égard de la sécurité physique des actifs informationnels sont les suivantes :

- connaître et mettre en œuvre, en collaboration avec le RLSI, les meilleures pratiques en matière de sécurité physique des actifs informationnels dans la conception, la réalisation ou la modification des processus d'affaires;
- prévoir, en collaboration avec le RLSI, toutes les mesures nécessaires pour la reprise du processus d'affaires.

Le personnel

Certaines personnes à l'emploi du Ministère sont particulièrement concernées par la sécurité physique des documents. Ce sont celles qui sont attitrées au classement (personnel de secrétariat, responsables de poste de classement, registraires des plans, etc.). Elles ont le devoir de veiller à la protection des documents utilisés dans leur secteur d'activités.

Pour l'ensemble du personnel, chacun est responsable d'assurer la sécurité physique des actifs informationnels mis à sa disposition par le Ministère. Les responsabilités de tout membre du personnel sont les suivantes :

- protéger les documents et les équipements informatiques en sa possession contre le vol ou toute autre forme de menace;
- protéger les renseignements confidentiels du ministère des Transports en sa possession en appliquant les mesures de sécurité physique appropriées au support d'information en cause;
- maintenir, peu importe son support physique, l'intégrité de l'information traitée dans le contexte de son travail;
- éliminer les supports de stockage de l'information - papier, microfilm et support électronique, magnétique, optique ou autre - en conformité avec les exigences du Ministère;
- informer son gestionnaire de tout événement ayant mis ou qui aurait pu mettre en péril la sécurité physique des actifs informationnels du Ministère;
- informer le STMU de tout incident lié de près ou de loin à la sécurité des actifs informationnels du Ministère.

Le Centre multiservices informatiques (CMI)

Les principales responsabilités du CMI sont les suivantes :

- enregistrer les incidents de sécurité physique réels ou présumés qui lui sont signalés et gérer le registre ministériel des incidents de sécurité. Le CMI demeure en contact permanent avec le Service des enquêtes et le responsable de la sécurité physique dans le but de garantir la prise en charge des incidents de sécurité physique.

Les intervenants responsables de la reprise

Les responsabilités des intervenants chargés de la reprise des systèmes de mission du ministère des Transports et des responsables de reprise des systèmes locaux (RLSI et STMU) sont les suivantes :

- prévoir et intégrer, lors de la mise en place des plans et procédures pour la reprise, en collaboration avec le RSP, toutes les mesures de sécurité physique appropriées pour garantir la disponibilité et l'intégrité des actifs informationnels nécessaires pour la reprise;
- s'assurer, lors des tests et essais de reprise, de l'application et de l'efficacité des mesures de sécurité physique.

La Direction de la planification et des stratégies de l'information (DPSI)

Les principales responsabilités de la DPSI sont les suivantes :

- élaborer, en collaboration avec le RSP, les éléments normatifs qui découlent de la présente directive;
- soutenir les intervenants, notamment les détenteurs et les gestionnaires, dans leurs efforts pour assumer les responsabilités à l'égard de la gestion de la sécurité physique des actifs informationnels;
- participer à la sensibilisation et à la formation du personnel à l'importance de la sécurité physique des actifs informationnels.

La Direction des systèmes et des technologies de l'information (DSTI)

Les principales responsabilités de la DSTI sont les suivantes :

- planifier et coordonner la mise en œuvre du plan de reprise des systèmes de mission du Ministère et s'assurer, en collaboration avec le RSP, de l'intégration et de la prise en considération des mesures de sécurité physique dans les tests et les essais de reprise;
- à l'égard de la gestion de la sécurité, soutenir les intervenants et, notamment, les détenteurs, les gestionnaires et les intervenants responsables de la reprise, dans leurs efforts pour assumer les responsabilités qui leur sont attribuées par le Registre d'autorité de la sécurité;
- réaliser la prise des copies de sécurité des serveurs ainsi que l'entreposage et la gestion sécuritaire des supports informatiques pour la reprise des systèmes de mission.

La Direction du secrétariat

À l'égard de la gestion de la sécurité de l'information et plus particulièrement en ce qui a trait à la protection des renseignements personnels, la Direction du secrétariat doit fournir l'encadrement juridique et l'expertise quant à l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Dans cet esprit, la Direction du secrétariat a la responsabilité suivante :

- collaborer, avec le RSP et les détenteurs, à la détermination des mesures de sécurité physique nécessaires pour assurer la protection des documents sur support physique - papier, audio ou vidéo, microfilm, etc. - ou sur des supports de stockage numériques qui contiennent des renseignements personnels.

La Direction de la vérification interne et de l'évaluation de programmes

Le Ministère a confié à la Direction de la vérification interne et de l'évaluation de programmes le mandat de vérifier si les règles relatives à la sécurité de l'information sont respectées. Dans ce contexte, la Direction a la responsabilité suivante :

- effectuer la vérification des activités et des pratiques de gestion du Ministère de façon à s'assurer que les mesures de sécurité physique des actifs informationnels sont prises en considération et appliquées en conformité avec les exigences énoncées par le Ministère.

Le Service des enquêtes

Le Service des enquêtes intervient pour évaluer un incident de sécurité physique concernant un actif informationnel et procéder aux enquêtes s'y rapportant. Dans ce contexte, les principales responsabilités du Service des enquêtes sont les suivantes :

- assurer la gestion du processus de déclaration des incidents de sécurité physique, en collaboration avec le CMI;
- analyser les incidents de sécurité physique en collaboration avec le RSP et découvrir les causes à leur origine;
- préciser et communiquer au RSIN et au RMS, en collaboration avec le RSP, les mesures de sécurité physique à mettre en place le cas échéant, pour éviter que ce type d'incident se reproduise, ainsi que les mesures à appliquer pour limiter les impacts dans l'éventualité où un tel incident se reproduirait.

La Direction des contrats et des ressources matérielles (DCRM)

Les principales responsabilités de la DCRM en ce qui concerne la sécurité physique des actifs informationnels dans les édifices centraux sont les suivantes :

- acquérir, mettre en place et exploiter les systèmes de contrôle des accès physiques;
- sélectionner, acquérir, mettre en place et exploiter les systèmes de soutien environnementaux assurant la sécurité des actifs informationnels – système CVCA[2], protection contre les incendies, génératrice de secours, alimentation électrique, etc;
- assurer l'adéquation des moyens matériels et environnementaux de protection aux besoins de sécurité physique des actifs informationnels;

2. Systèmes de chauffage, de ventilation et de climatisation d'air, systèmes d'alimentation électrique, etc.

- gérer et mettre en œuvre les services de gardiennage et d'accueil nécessaires pour assurer la protection des actifs informationnels;
- assurer la réalisation matérielle des recommandations en matière de sécurité physique;
- assurer l'élimination[3] et, en particulier, la destruction sécuritaire des actifs informationnels à protéger, notamment du matériel informatique et des supports de stockage de l'information - papier, microfilm et support électronique, magnétique, optique ou autre ou faisant appel à une combinaison de technologies.

La DCRM peut également assister, sur demande, les directions territoriales dans l'exécution de ces tâches.

La Direction des ressources humaines (DRH)

La principale responsabilité de la DRH est la suivante :

- participer à la sensibilisation et à la formation du personnel à propos de l'importance de la sécurité physique des actifs informationnels.

3. Pour la procédure de disposition des biens excédentaires lies aux technologies de l'information, il faut se référer à la directive 2.5.1 (Volume II) du *Manuel administratif* du ministère des Transports.

Transports Québec