

AIDE-MÉMOIRE



Mesures de sécurité physique des installations

Juin 2019

Table des matières

Destinataires de ce document.....	3
Sécurité physique – Raisons d’être, principes et objectifs.....	3
Actifs à protéger	3
Mise en application	3
Principes de prévention du crime	3
Prévention du crime par l’aménagement du milieu (PCAM).....	4
Enveloppe du bâtiment – protection des ouvertures	5
Contrôle des accès	5
Système d’alarme	6
Vidéosurveillance	7
Conseils lors de l’acquisition	7
Informations supplémentaires	8

Destinataires de ce document

Le document est destiné aux petites et moyennes entreprises (PME) voulant mettre en place des mesures de sécurité physique pour protéger leurs actifs.

Ce document ne contient pas une liste exhaustive, mais un résumé des points principaux à examiner et à prendre en compte lors de l'élaboration d'un plan de sécurité physique pour une organisation.

Toutes les mesures et procédures de sécurité physique doivent respecter les lois et codes en vigueur.

Sécurité physique – Raisons d'être, principes et objectifs

La sécurité physique est l'ensemble des mesures de sécurité conçues pour protéger les actifs (les renseignements, les biens et les installations) contre l'accès, la divulgation, la modification ou la destruction non autorisés, en fonction de leur niveau de sensibilité, de leur pertinence et de leur valeur.

La valeur d'un actif correspond au degré de préjudice qui résulterait d'une atteinte à l'intégrité, à l'accessibilité et à la disponibilité de l'actif.

Actifs à protéger

Les actifs peuvent se retrouver sous différentes formes :

- Tangibles (ex. : équipements ayant une grande valeur)
- Intangibles (ex. : propriété intellectuelle, informations confidentielles)
- Mixtes (ex. : employés)

Mise en application

Chaque organisation peut appliquer différemment les mesures de sécurité à adopter en suivant cette démarche :

1. Identifier les actifs
2. Déterminer la valeur des actifs
3. Prioriser les actifs selon leur valeur
4. Déterminer les menaces et vulnérabilités pour chaque actif
5. Déterminer les mesures à mettre en place pour chaque actif

Principes de prévention du crime

La mise en place de mesures et systèmes de protection physiques doit être effectuée selon des principes de prévention du crime.

Principes	Objectifs
Dissuader	Créer un environnement qui démontre que le risque d'échec d'une attaque est plus grand que la réussite de l'objectif poursuivi par l'attaquant.
Détecter	<ul style="list-style-type: none"> • Détecter une attaque en cours • Aviser une équipe d'intervention
Retarder	Ralentir les acteurs malveillants dans l'atteinte de leur objectif afin de permettre une réponse appropriée à l'attaque.
Empêcher	Empêcher les acteurs malveillants d'atteindre leur objectif <ul style="list-style-type: none"> • Par des mesures efficaces qui ont dissuadé les acteurs malveillants • Par des interventions dans un délai approprié selon le type d'attaque

Prévention du crime par l'aménagement du milieu (PCAM)

La prévention du crime par l'aménagement du milieu propose l'utilisation efficace de l'environnement pour garder les intrus en observation afin de réduire les opportunités criminelles et protéger les occupants légitimes. Le PCAM repose sur des principes applicables aux bâtiments et à leur environnement extérieur.

Principes :

Surveillance naturelle

Maximiser la visibilité (voir et être vue) à partir des espaces publics environnants.

- Voir de l'extérieur vers l'intérieur du bâtiment
- Voir de l'intérieur vers l'extérieur du bâtiment
- L'environnement extérieur entourant le bâtiment

Contrôle d'accès naturel

- Diriger les personnes et véhicules vers des points d'accès spécifiques
- Décourager ou empêcher les accès à l'aide de barrières physiques ou symboliques (signalisation)

Renforcement territorial et définition des limites

- Distinguer clairement les zones publiques de celles privées
- Créer un sentiment d'appartenance pour les utilisateurs et occupants légitimes
- Augmenter la vigilance des utilisateurs légitimes à repérer les acteurs malveillants
- Indiquer aux acteurs malveillants qu'ils ne sont pas les bienvenus (dissuasion)

Démontrer que l'espace est occupé

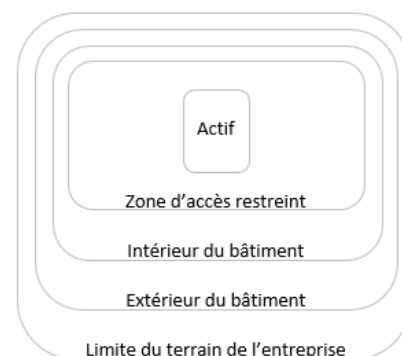
- Inciter les activités légitimes sur les lieux
- Démontrer que l'espace est surveillé
- Démontrer une présence constante
- Assurer une maintenance des lieux

Éclairage sécuritaire (intérieur/extérieur)

- Chevaucher l'éclairage dans le but de réduire les espaces non éclairés
- Uniformiser l'éclairage d'une zone à l'autre
- Limiter les effets d'éblouissement

Défense en profondeur

- Créer plusieurs couches de protection
- Protéger les actifs critiques derrière plusieurs barrières
- Augmenter le temps nécessaire pour la commission d'une attaque
- Bâtir une stratégie de défense reposant sur plusieurs mesures différentes qui se complètent
- Donne le temps nécessaire pour une intervention



Enveloppe du bâtiment – protection des ouvertures

La plupart des intrusions dans les bâtiments se font par les portes et les fenêtres. Si possible, les ouvertures devraient offrir une résistance qui tend à être équivalente à celle des murs.

Types d'ouverture :

- Portes (quincaillerie, matériaux de la porte et du cadre, etc.)
- Fenêtres (type de verre, pellicule anti-bris, barreaux, etc.)
- Autres ouvertures (persienne de ventilation, trappe, etc.)

Contrôle des accès

Technique regroupant différentes méthodes qui consiste à soumettre l'entrée d'un établissement ou de locaux à une autorisation d'accès afin de protéger les personnes, les informations et les biens.

Le contrôle d'accès peut s'appliquer :

- Au personnel de l'entreprise, aux visiteurs et aux fournisseurs
- À certains membres du personnel pour certains lieux sensibles (bureaux, salles informatiques)
- À toutes les heures ou à certaines heures de la journée ou de la nuit
- À des personnes, des véhicules, des marchandises

Principes de contrôle des accès

- Réduire au maximum la quantité de points d'entrée pour faciliter le contrôle des accès
- Délimiter clairement les points d'entrée par un périmètre facile à reconnaître comme une porte ou des meubles disposés d'une façon particulière
- Contrôler l'accès à tous les points d'entrée pour filtrer les gens et le matériel qui entrent

Méthodes de contrôle des accès

- Reconnaissance personnelle (réceptionniste, agent de sécurité, collègue)
- Mécanique (serrure à combinaison ou à usage d'une clé contrôlée ou non)
- Électronique (carte d'accès, clavier, biométrie)

Gestion des droits d'accès

Afin d'assurer une gestion sécuritaire des accès physiques, l'accès à une zone ou à un actif devrait seulement être accordé lorsque la fonction de la personne l'exige, et ce, sans égard au statut hiérarchique de la personne.

Gestion des dispositifs d'accès

Un dispositif d'accès donne le droit au détenteur d'entrer la zone contrôlée (code, clé, carte, etc.)

- Limiter la quantité de dispositifs d'accès en circulation au minimum
- Conserver les dispositifs dans une armoire verrouillée et limiter l'accès aux personnes responsables d'octroyer les dispositifs d'accès
- En cas de perte, vol ou compromission, recoder (réinitialiser) les serrures et désactiver la carte
- Tenir à jour un registre des dispositifs d'accès octroyés et en conservation
- Effectuer une révision périodique des dispositifs d'accès octroyés
- Effectuer une révision des dispositifs d'accès octroyés lors d'une cessation d'emploi, fin de contrat ou changement de fonction

Gestion des visiteurs

Des procédures de contrôle d'accès doivent aussi être mises en place pour les visiteurs. Un visiteur est une personne qui n'est pas un employé de l'organisation et qui doit accéder à une zone réservée aux employés. L'objectif est d'empêcher un visiteur d'accéder à une zone à accès restreint sans autorisation.

- Établir une procédure d'identification et d'accompagnement des visiteurs
- Maintenir un registre d'entrées et de sorties pour les visiteurs

Système d'alarme

Le système d'alarme est une mesure visant à détecter et communiquer en temps réel des activités anormales :

- Détection d'intrusion périmétrique (contacts de portes, etc.)
- Détection d'intrusion volumétrique (détecteurs de mouvement, etc.)
- Détection d'incendie et gaz
- Alerte d'aide à la personne (urgence médicale, agression, etc.)
- Supervision de points critiques (température, niveau d'eau, etc.)

Bonnes pratiques

- Établir des procédures de réponse aux alarmes en fonction des types d'alarmes
- Avoir un système qui offre une protection d'au moins 24 heures en cas de panne de courant
- Limiter la quantité d'utilisateurs du système d'alarme au minimum
- Retirer tous les utilisateurs qui ne sont plus nécessaires lors d'une cessation d'emploi
- Assigner des niveaux d'autorité en fonction des tâches à accomplir
- Doter le système d'alarme de deux modes de communication avec la centrale de réception des alarmes
- Effectuer une mise à l'essai périodique du système d'alarme
- Installer des sirènes à l'intérieur

Vidéosurveillance

La vidéosurveillance peut constituer un élément précieux du programme de sécurité d'un établissement. La surveillance vidéo est principalement utilisée pour:

- Détecter les activités qui appellent une réponse de sécurité
- Recueillir des images d'un incident pour un examen ultérieur et les utiliser comme preuves si nécessaire
- Aider à l'évaluation d'un incident

Les exigences fonctionnelles d'un système de vidéosurveillance peuvent être déterminées en répondant aux questions suivantes:

- Quel est le but du système?
- Qu'est-ce que chaque caméra doit voir?
- Quelles sont les exigences pour la surveillance en temps réel ou l'enregistrement des images?
- Quelles sont les contraintes d'éclairage?

Vidéosurveillance et protection des renseignements personnels

Les images et autres informations captées par un système de vidéosurveillance constituent des renseignements personnels au sens de la Loi. La vidéosurveillance étant une forme d'intrusion à la vie privée, son utilisation impose certaines obligations relatives à la cueillette et à la conservation de renseignements personnels.

Conseils lors de l'acquisition

Voici quelques notions importantes lorsque vient le temps de faire une soumission auprès d'un fournisseur de services de sécurité.

- Demander une soumission ventilée (pièces, main d'œuvre, déplacement, frais annuels, etc.)
- Demander des plans indiquant l'emplacement des composantes
- Acheter des équipements pouvant être supportés par plusieurs fournisseurs afin qu'il soit possible de changer de fournisseur sans avoir à remplacer son équipement
- Se renseigner sur les délais de service en cas de défectuosité

Informations supplémentaires

Pour plus d'informations, vous pouvez consulter ces références :

- *Manuelle de la sécurité industrielle*, gouvernement du Canada : <https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-fra.html>
- *Ressources du manuel de sécurité industrielle*, gouvernement du Canada : <https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/rssrcs-rsrcs-fra.html#s1>
- *G1-025 Protection, détection et intervention*, Gendarmerie royale du Canada : <http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-025-fra.htm#7.1>
- Asis : <https://www.asisonline.org/>