McGill Security Services | Service de sécurité

Protocole d’installation des dispositifs de sécurité

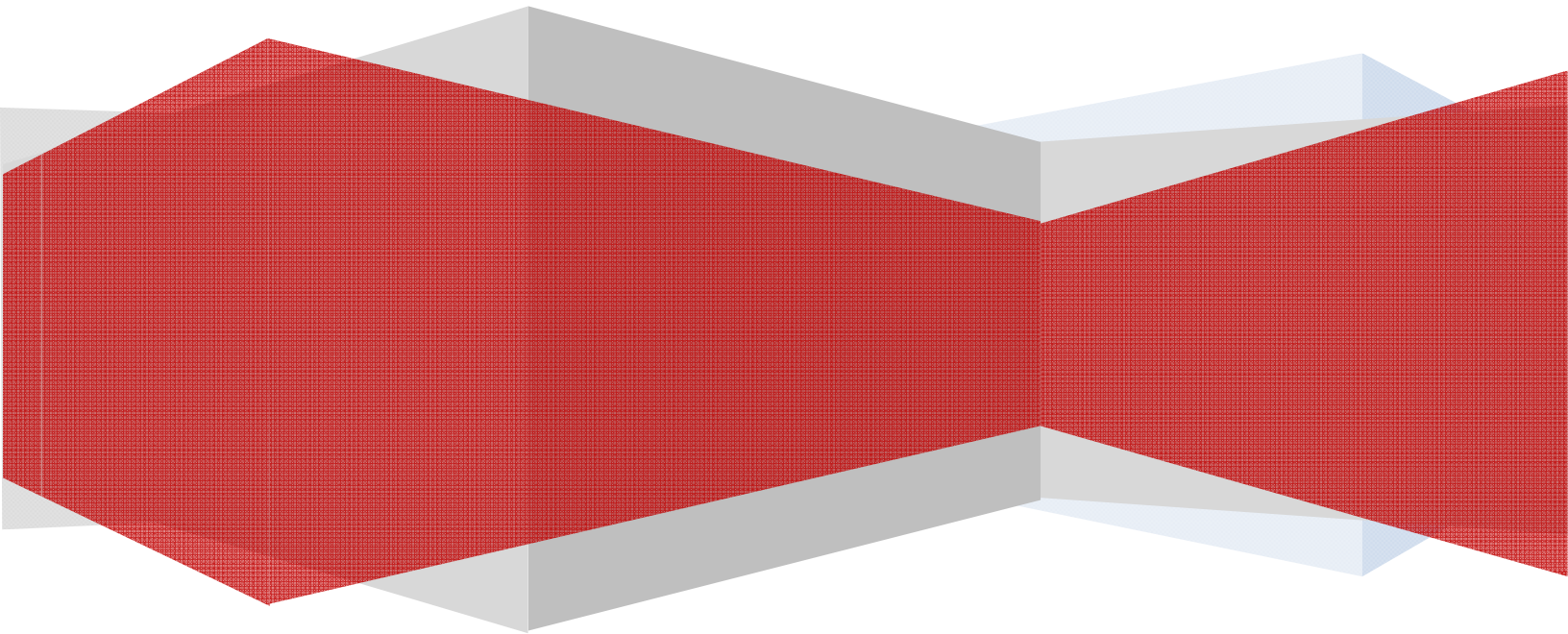

TABLE DES MATIÈRES

1.0 BUT

1.1 Le Service de sécurité de l'Université McGill administre le système central de sécurité de l'Université, incluant la surveillance des alarmes, le système de contrôle d'accès par carte et le réseau de caméras de sécurité. Pour que le système soit efficient et efficace, les dispositifs de sécurité doivent être installés et utilisés selon les normes établies et les meilleures pratiques connues.

1.2 La protection des biens doit être économique. On pourrait croire que la sécurité des personnes et la protection des biens dépendent de l'installation d'un grand nombre de systèmes et dispositifs de sécurité. C'est faux, un système ou dispositif de sécurité n'est efficace que s'il est utilisé adéquatement. Il ne faut jamais penser qu'un dispositif de sécurité puisse remplacer la diligence et la prudence des personnes.

1.3 Le protocole présenté dans ce document a deux (2) objectifs :

1.3.1 l'établissement d'un processus et de normes cohérentes pour régir la sélection, l'acquisition, l'installation et le fonctionnement des dispositifs de sécurité qui favorisent le maintien d'un milieu sûr à l'Université McGill.

1.3.2 la réduction de la fréquence des fausses alarmes causées par des problèmes d'installation. Les fausses alarmes nuisent à l'efficacité du système et augmentent les coûts de fonctionnement.

2.0 PORTÉE

2.1 Ce protocole s'applique à tous les sites présents et futurs de l'Université sous la responsabilité fonctionnelle du Service de sécurité, y compris les projets de nouvelle construction et de rénovation des immobilisations.

2.2 Il vise tout espace loué par l'Université où le dispositif de sécurité est surveillé par le Service de sécurité.

2.3 Ce protocole ne s'applique pas aux :

2.3.1 systèmes de protection incendie – ils sont administrés par le Bureau des mesures d'urgence et de prévention des incendies;

2.3.2 alarmes de détecteur de conditions ambiantes – l'installation de détecteurs de conditions ambiantes n'est pas soumise à l'approbation du Service de sécurité.

3.0 DÉFINITIONS

3.1 Abonné – service, faculté, département de l'Université ou entité externe à McGill qui possède un dispositif de sécurité; ou la personne chargée de gérer un dispositif de sécurité. L'abonné qui gère un lecteur de cartes porte le titre de gestionnaire d'accès.

3.2 Alarme anti-hold-up – bouton d'alarme activé lorsqu'une tentative de hold-up ou un hold-up (vol) est perpétré. L'utilisation de l'alarme anti-hold-up est réservée aux endroits où il y a des caisses enregistreuses, là où on manipule de l'argent. Voir aussi : Alarme de panique.

3.3 Alarme anti-intrusion – système utilisant des détecteurs de mouvement, des contacts de porte/fenêtre et autres dispositifs pour détecter une entrée non autorisée dans un secteur protégé. Un signal est envoyé au Centre opérationnel du Service de sécurité lorsque cela se produit.

3.4 Alarme de panique – bouton d'alarme utilisé dans des endroits où peuvent se produire une situation constituant un danger de mort, une urgence médicale ou autre situation exigeant une intervention immédiate. Les alarmes de panique sont habituellement installées à des points de service à la clientèle; des alarmes portatives sont aussi disponibles. Voir aussi : Alarme anti-hold-up pour les comptoirs de transactions en argent comptant.

3.5 Appel de vérification amélioré – procédure de vérification du Centre opérationnel du Service de sécurité qui effectue deux appels téléphoniques à deux personnes désignées d'avance, avant d'envoyer une patrouille de sécurité pour répondre à une alarme. Si une personne contact répond qu'il s'agit d'une erreur et confirme son identité au moyen d'un mot de passe, le problème est réglé et aucune patrouille n'est envoyée.

3.6 Carte de proximité – nom générique de dispositifs en circuit intégré sans contact utilisés pour sécuriser les accès. L'Université McGill utilise trois types de cartes de proximité : (1) la carte d'étudiant et d'employé de McGill avec photo; (2) la carte vierge de proximité pour les employés temporaires et les visiteurs; et (3) la carte d'identité des fournisseurs de services à McGill pour les employés d'entreprises liées par contrat à l'Université.

3.7 Centre opérationnel du Service de sécurité – principale station de surveillance des alarmes à l'Université, il y en a une sur chaque campus (centre-ville et Macdonald).

3.8 Clavier - périphérique qui permet à l'utilisateur d'entrer un code numérique ou une clé, ou qui scanne un dispositif de proximité comme une carte ou une breloque, pour armer (allumer) ou désarmer (éteindre) le système d'alarme anti-intrusion.

3.9 Contact de porte/fenêtre – capteur posé dans le cadre ou à la surface d'une porte ou fenêtre. Le capteur fait partie du système d'alarme anti-intrusion. Il détecte l'ouverture et la fermeture de la porte ou la fenêtre, et déclenche un signal d'alarme en cas d'entrée ou de sortie non autorisée.

3.10 Demandeur – personne qui demande l'installation d'un dispositif de sécurité. Il peut s'agir de l'utilisateur final ou d'une personne qui représente l'utilisateur final (p. ex. gestionnaire de projet, administrateur de service, faculté ou département, ou directeur d'immeuble).

3.11 Détecteur de bris de vitre – type de capteur conçu pour détecter le son particulier d'un bris de vitre dans le secteur protégé.

3.12 Détecteur de mouvement - dispositif détectant le mouvement dans un secteur protégé. Le détecteur de mouvement est connecté au panneau d'alarme anti-intrusion et fait partie du système d'alarme anti-intrusion.

3.13 Détecteur d'ouverture d'issue – détecteur de mouvement utilisé pour permettre un moyen d'évacuation par une porte protégée par un signal d'alarme, sans déclencher l'alarme.

3.14 Gestionnaire d'accès (« Area Access Manager – AAM ») – personne désignée par un service, un département ou une faculté pour gérer ses lecteurs de cartes avec le pouvoir d'accorder ou de retirer au détenteur de carte l'accès aux secteurs sous sa responsabilité; et de fixer et modifier les réglages des lecteurs de cartes. Le gestionnaire d'accès reçoit une formation particulière du Service de sécurité. Un gestionnaire d'accès est distinct d'un abonné bien que la même personne puisse jouer les deux rôles.

3.15 Languette d'ordinateur personnel et de podium - type de capteur constitué d'une boucle de fibre optique formant un circuit, généralement utilisé pour prévenir le vol d'appareils onéreux dans une zone protégée. La boucle est attachée à l'appareil et lorsque celui-ci est enlevé, le circuit se brise et l'alarme est déclenchée

3.16 Lecteur de cartes – dispositif électronique qui peut lire un insigne d'identité comme une carte de proximité, vérifier les droits d'accès associés à cet insigne et déverrouiller les portes, ou faire fonctionner les ascenseurs lorsque les droits d'accès sont valides. C'est un dispositif à double usage. Voir aussi : Système à double usage.

3.17 Mot de passe – code alphanumérique utilisé pour identifier les utilisateurs lorsqu'ils appellent le Service de sécurité.

3.18 Partition – groupe de zones à l'intérieur d'un système d'alarme anti-intrusion plus étendu qui permet d'armer ou de désarmer de façon indépendante un certain nombre de secteurs à partir d'un panneau unique d'alarme anti-intrusion. En raison de nombreuses erreurs des utilisateurs, le Service de sécurité ne permet pas de nouvelles installations avec des partitions.

3.19 Système à double usage - système électronique tel un lecteur de cartes qui a la double fonction de contrôle d'accès et d'alarme anti-intrusion.

3.20 Système de contrôle d'accès – dispositif ou système électronique qui restreint l'accès physique et l'entrée aux personnes autorisées. Ce type de système est utilisé dans les

secteurs fréquentés par un grand nombre d'utilisateurs autorisés à toute heure du jour ou de la nuit. Un système de contrôle d'accès remplace habituellement le système traditionnel de serrures et clés.

3.21 Utilisateurs – membres de la collectivité de McGill qui fréquentent un secteur, qui y travaillent ou y étudient, ou qui sont autorisés à accéder au secteur protégé au moyen du dispositif de sécurité installé par le service, la faculté ou le département propriétaire.

3.22 Zone – zone particulière à l'intérieur d'un secteur protégé par le système d'alarme anti-intrusion. Les normes en vigueur ne permettent qu'un seul capteur par zone pour la sécurité des intervenants et pour améliorer la capacité de diagnostique. Cette restriction ne s'applique pas aux languettes d'ordinateur personnel et de podium.

4.0 PROTOCOLE

4.1 Généralités

4.1.1 Tous les dispositifs de sécurité installés dans les endroits sous le contrôle de l'Université McGill, doivent être approuvés par le Service de sécurité.

4.1.2 Le cas échéant, tous les dispositifs de sécurité installés dans un immeuble de McGill doivent être approuvés par le directeur d'immeuble.

4.1.3 Là où ils ne sont pas couverts par le contrat de location, tous les dispositifs de sécurité installés dans un local commercial loué par l'Université, doivent être approuvés par le locateur.

4.1.4 Nul dispositif de sécurité dans un lieu sous le contrôle de l'Université McGill ne sera enlevé sans l'approbation expresse du Service de sécurité.

4.1.5 L'installation de tout dispositif de sécurité dans un lieu sous le contrôle de l'Université McGill, doit être faite par les Services de réseaux et communications (Network Communications Services – NCS) ou un entrepreneur qualifié approuvé par NCS.

4.1.6 Pour investiguer plus facilement les alarmes, les numéros de locaux de tous les secteurs protégés par un dispositif de sécurité doivent être affichés à un endroit visible en tout temps.

4.1.7 L'accès à tous les secteurs protégés par des dispositifs de sécurité ou du matériel d'alarme doit être accordé au Service de sécurité par l'abonné pour que les intervenants du Service de sécurité puissent investiguer toute possibilité de crime en cours. Là où l'accès au secteur est restreint pour des raisons de sécurité, un autre protocole d'intervention doit être établi.

4.2 Procédure de demande

4.2.1 Les demandeurs qui désirent installer un dispositif de sécurité doivent remplir un *Formulaire de demande de dispositif de sécurité* en ligne sur le site Web du Service de sécurité. Les gestionnaires de projet peuvent communiquer directement avec le Service de sécurité.

4.2.2 Le Service de sécurité procède à une inspection sur place pour évaluer les besoins du demandeur en matière de sécurité et déterminer la meilleure solution. L'inspection examine la sécurité du secteur, du personnel, des intervenants en réponse à une alarme et les technologies actuelles dans le domaine des alarmes. Suite à l'inspection, le Service de sécurité recommande parfois une solution autre que celle envisagée au départ.

4.2.3 L'inspection des lieux peut inclure une consultation auprès des Services de réseaux et communications, du Bureau de gestion et développement des installations et du Bureau de prévention des incendies. Cette inspection peut nécessiter environ une à deux semaines.

4.2.4 Le Service de sécurité demande ensuite une proposition de prix des Services de réseaux et communications pour l'installation du dispositif requis. Les Services de réseaux et communications doivent obtenir une estimation de Gestion et développement des installations pour toute modification nécessaire à la quincaillerie. Cette procédure peut prendre jusqu'à quatre semaines pour les installations régulières et un délai plus long pour les installations sur mesure. Le Service de sécurité envoie ensuite l'estimation au demandeur pour approbation.

4.2.5 Si le demandeur approuve le prix proposé, il doit fournir un numéro FOAPAL ou numéro de client pour la facturation. Le demandeur est ensuite avisé du délai requis pour l'installation et la programmation du dispositif demandé. Le délai d'installation varie et peut être plus long s'il faut procéder à l'achat de quincaillerie spéciale.

4.2.6 Pour les grands projets de rénovation et de construction, le Service de sécurité demande un avis de soixante (60) jours avant la date de livraison anticipée.

4.2.7 Au cours du processus d'installation, le demandeur doit désigner au moins deux (2) abonnés qui recevront une formation du Service de sécurité pour assumer la responsabilité du dispositif.

4.2.8 Après l'installation du dispositif, le Service de sécurité le configure et avise l'abonné lorsque le dispositif est prêt à entrer en fonction.

4.3 Lecteurs de cartes

4.3.1 Un lecteur de cartes est avant tout un dispositif de contrôle d'accès. Il est suggéré aux demandeurs qui désirent un dispositif de sécurité pour protéger des

biens précieux, d'acquérir un système d'alarme anti-intrusion contrôlé par clavier et surveillé 24 heures sur 24, 7 jours sur 7.

4.3.2 La porte sur laquelle il faut poser le lecteur de cartes doit respecter les exigences suivantes :

i. la porte doit être en bon état et convenir à l'installation d'un système de lecteur de cartes;
ii. la porte doit être munie d'un ferme-porte sans rallonge;
iii. la porte doit être munie d'un dispositif de détection de sortie;
iv. les gâches électriques doivent être du type « serrure à fermeture en cas de panne de courant »; ainsi, lorsque le dispositif de sortie de secours est activé, il ne passe outre qu'au contact de porte sans déverrouiller la porte; et
v. la porte doit être munie d'un cylindre Medeco à goupille sur une entrée de clé homologuée exclusive au Service de sécurité, pour que les utilisateurs ne puissent contourner le lecteur de cartes avec une clé.

4.3.3 Si le demandeur ne veut pas de service de surveillance d'alarmes pour le lecteur de cartes, le ferme-porte et le dispositif de détection de sortie peuvent ne pas être nécessaires.

4.3.4 Le Service de sécurité surveille les alarmes de lecteurs de cartes en accord avec son *Protocole de surveillance des alarmes de sécurité*, dont une copie est remise au client au cours de l'installation.

4.4 Systèmes anti-intrusion et composantes

4.4.1 Lorsqu'un système d'alarme anti-intrusion est demandé pour un secteur, ce dernier doit respecter les exigences suivantes :

i. les portes doivent être en bon état et convenir à l'installation de contacts de porte ou autres dispositifs;
ii. les fenêtres doivent être en bon état et convenir à l'installation de contacts ou détecteurs de bris de vitre; et
iii. les meubles ne doivent pas obstruer les détecteurs de mouvement.

4.4.2 Les normes suivantes s'appliquent à tous les systèmes d'alarme anti-intrusion installés à l'Université McGill :

i. un clavier doit être installé à chaque entrée utilisée pour pénétrer dans un secteur protégé;
ii. chaque type d'alarme (intrusion, trouble inconnu, sabotage, pile faible) doit émettre un signal pour une zone distincte;
iii. le détecteur de bris de vitre doit être relié à un système anti-intrusion avec clavier;
iv. chaque capteur anti-intrusion doit émettre un signal pour une zone distincte à moins d'indication contraire du Service de sécurité, on ne fera exception que pour des dispositifs du même type dans la même pièce;

v. les zones doivent être clairement indiquées par des étiquettes sur le clavier numérique;
vi. une sirène audible pendant au moins une minute est requise pour tous les systèmes de détection d'intrusion;
vii. le clavier doit émettre un son audible pour avertir l'utilisateur que le cycle de temporisation de sortie (« exit delay ») est commencé; et
viii. le clavier doit émettre un son audible pour avertir l'utilisateur d'une erreur de sortie (« exit error fault ») commise en armant le système d'alarme ou en quittant le secteur protégé.

4.4.3 Le Service de sécurité surveille les systèmes d'alarme anti-intrusion conformément à son *Protocole de surveillance des alarmes de sécurité*, dont une copie est remise à l'abonné au cours de l'installation.

4.5 Languettes d'ordinateur personnel et de podium

4.5.1 L'installation de languettes d'ordinateur et de podium doit toujours faire partie d'un système de sécurité plus complet comprenant aussi des mécanismes de verrouillage, lecteurs de cartes, caméras de sécurité, etc.

4.5.2 Les languettes d'ordinateur personnel et de podium doivent être reliées à une sirène.

4.5.3 Toute pièce où il y a plus de cinq (5) languettes doit être munie d'un panneau d'alarme géré par l'abonné.

4.5.4 À remarquer qu'une languette de sécurité est automatiquement apposée à tous les rétroprojecteurs et téléviseurs à écran plat installés par les Services multimédia des Services de réseaux et communications.

4.6 Caméras vidéo

4.6.1 L'installation de caméras et l'accès aux images en direct et enregistrées sont régis par le *Protocole d'utilisation des caméras en circuit fermé* (*CCTV Protocol*).

4.6.2 Les lieux d'installation de caméras extérieures sur le campus du centre-ville doivent être approuvés par les Services de conception.

4.7 Alarmes anti-hold-up et alarmes de panique

4.7.1 Les alarmes anti-hold-up et alarmes de panique ne doivent jamais être considérées comme solution unique à un risque pour la sécurité. Elles doivent toujours être assorties à d'autres mesures de sécurité prises en fonction de ce risque.

4.7.2 On encourage fortement les utilisateurs d'alarmes anti-hold-up et alarmes de panique à suivre la formation sur l'intervention non violente en situation de crise

(*Non-violent Crisis Intervention®*) offerte par le Service de sécurité.

4.7.3 Tous les utilisateurs d'alarmes de panique doivent avoir un mot de passe pour s'identifier en cas d'appel au Service de sécurité pour une fausse alarme.

4.7.4 L'abonné qui demande une alarme de panique doit aussi installer une caméra de surveillance ou fournir au moins deux numéros de téléphone de personnes à contacter sur les lieux en plus de l'utilisateur de l'alarme de panique, pour permettre au Centre opérationnel du Service de sécurité de confirmer la nature de l'urgence pendant que la patrouille de sécurité est en route.

4.7.5 Une alarme de panique non surveillée par le Service de sécurité et conçue de façon à demander uniquement l'aide du personnel local, n'est pas soumise aux exigences mentionnées ci-dessus.

4.7.6 L'utilisation de l'alarme anti-hold-up est réservée aux endroits où il y a des caisses enregistreuses et là où on manipule de l'argent, elle doit avoir pour complément une caméra de surveillance.

4.8 Services de soutien, réparation et entretien

4.8.1 *L'Engagement au niveau de service pour les dispositifs de sécurité (Service Level Commitment for Security Devices)* contient une liste complète des services de soutien fournis aux abonnés des systèmes d'alarme et décrit les responsabilités des abonnés. Ceux-ci reçoivent une copie de ce document au cours de l'installation.

4.8.2 Toute nouvelle installation par les Services de réseaux et communications ou leurs entrepreneurs engagés, porte une garantie de douze mois sur les pièces et la main-d'œuvre à partir de la date d'achèvement de l'installation. Après cette période de garantie, les réparations et pièces de remplacement sont aux frais des propriétaires des composantes périphériques.

4.8.3 Lorsque les intervenants constatent une défectuosité du matériel, le Service de sécurité soumet la commande de travail aux Services de réseaux et communications au nom de l'abonné. Les réparations facturables ne seront pas exécutées sans l'approbation du client.

4.9 Mise hors service et enlèvement

4.9.1 Les abonnés qui désirent se défaire de leur dispositif de sécurité doivent soumettre leur demande au Service de sécurité. La procédure est semblable à celle de la demande d'installation.

4.9.2 Lorsqu'une unité déménage d'un espace commercial loué, et qu'aucune autre unité de McGill ne doit y emménager, la mise hors service et l'enlèvement des dispositifs de sécurité, si requis par le propriétaire, doivent faire partie du projet

de déménagement au même titre que toute autre réparation à effectuer aux murs, portes, etc. Ces travaux doivent être coordonnés avec le représentant du propriétaire des lieux.

4.9.3 Lorsqu'une unité déménage d'un local du campus et ne veut pas transférer les dispositifs de sécurité à ses nouveaux locaux :

i. la mise hors service et l'enlèvement des dispositifs de sécurité doivent faire partie du projet de déménagement, à moins que le prochain occupant s'engage formellement à utiliser les dispositifs en place; mais
ii. si le prochain occupant n'est pas encore connu, le projet de déménagement doit prévoir l'enlèvement des dispositifs même si ceux-ci restent en place jusqu'à ce que le nouvel occupant prenne une décision finale.

4.9.4 La stipulation ci-dessus s'applique aux lecteurs de cartes. À la demande du gestionnaire de projet (Gestion et développement des installations), les lecteurs de cartes ne seront plus transférables lors du déménagement d'une unité d'un espace du campus puisqu'il n'y a pas d'économie de coûts. Les unités qui déménagent se verront accorder le financement de nouveaux lecteurs de cartes.

5.0 RESPONSABILITÉS

5.1 Le Service de sécurité fournit des avis d'expert sur la prévention des pertes et la gestion des risques liés à la criminalité. Nous élaborons et appliquons des normes concernant les dispositifs de sécurité mis en place sur le campus, nous approuvons leur installation et leur enlèvement, et nous sommes responsables de la gestion et du fonctionnement de la station centrale de surveillance des alarmes.

5.2 Les Services de réseaux et communications sont responsables de l'installation et l'entretien des dispositifs de sécurité qui sont surveillés par la station centrale de surveillance des alarmes à l'Université. Ils ont aussi la responsabilité de l'achat de tous les dispositifs de sécurité et des périphériques requis et approuvés conformément aux normes établies.

6.0 ANNEXES

Annexe A FAQ – Lecteurs de cartes
Annexe B FAQ – Systèmes anti-intrusion et composantes
Annexe C FAQ – Languettes d'ordinateur personnel et de podium
Annexe D FAQ – Caméras de sécurité
Annexe E FAQ – Alarmes anti-hold-up et alarmes de panique

FAQ – Lecteurs de cartes

1. Quel type de local devrait être muni d'un lecteur de cartes?

Tout laboratoire, immeuble ou local peut avoir un lecteur de cartes. En gros, un lecteur de cartes peut être posé partout où il faut protéger un espace. Les lecteurs de cartes remplacent les systèmes de clés qui peuvent facilement être copiées ou perdues, ce qui représente un risque pour la sécurité. Les lecteurs de cartes utilisent des insignes d'identité déjà en usage à McGill et permettent aux administrateurs d'accorder ou de retirer en tout temps le droit d'accès aux utilisateurs, et aussi de déterminer l'accès au secteur à certaines périodes.

2. Où peut-on trouver plus d'information au sujet de l'installation d'un lecteur de cartes?

Veuillez consulter l'article 1891 de la Base de connaissances TI à http://www.mcgill.ca/it/.

3. Quel sera le coût?

Le coût sera déterminé par les Services de réseaux et communications après l'inspection de sécurité. On peut obtenir une approximation du coût en consultant l'article 1865 de la Base de connaissances TI à http://www.mcgill.ca/it/.

4. Sera-t-il possible de travailler dans le secteur durant l'installation du lecteur de cartes?

Oui.

5. L'installation d'un lecteur de cartes signifie-t-elle l'élimination des clés?

Oui. Les serrures seront changées et les clés ne pourront plus être utilisées. Tous les individus détenant des clés doivent recevoir un droit d'accès sur leur insigne d'identité. Seul le Service de sécurité aura une clé d'accès pour les situations d'urgence.

6. Un lecteur de cartes élimine-t-il le besoin d'autres dispositifs de sécurité à l'intérieur du secteur protégé?

Un lecteur de cartes sert principalement au contrôle d'accès. Si vous désirez protéger les biens à l'intérieur, l'inspection de sécurité recommandera les options disponibles.

7. Le Service de sécurité surveille-t-il les alarmes de lecteurs de cartes?

Veuillez consulter le *Protocole de surveillance des alarmes de sécurité.*

8. Puis-je demander un relevé pour voir qui a accédé à mon secteur?

Pour certaines zones d'accès restreint, surtout celles qui sont visées par des règlements gouvernementaux, des relevés de lecteur de cartes peuvent être produits régulièrement. Pour tous les autres secteurs, les demandes de relevés de lecteur de cartes doivent être motivées. Les demandeurs doivent inclure tous les détails pertinents au motif invoqué pour obtenir l'approbation de la demande sans délai. Cette précaution est prise pour empêcher tout usage abusif d'un dispositif de sécurité. Par exemple, une demande de relevé de lecteur de cartes ne sera pas approuvée si le demandeur veut l'utiliser pour confirmer les heures travaillées ou la présence au travail. Une telle demande devrait être accompagnée de l'approbation des Ressources humaines. De la même façon, une demande de relevé de lecteur de cartes ne sera pas approuvée si le demandeur entend l'utiliser dans le cadre d'une enquête criminelle, car une telle enquête relève du Service de sécurité.

9. Que se passe-t-il en cas de panne de courant? Mon lecteur de cartes peut-il fonctionner?

Oui, il peut fonctionner. Les lecteurs de cartes sont tous munis de piles de secours qui permettent au lecteur de cartes de fonctionner pendant un certain nombre d'heures selon le nombre de dispositifs de sécurité et de panneaux dans l'immeuble. Lorsque les piles de secours sont épuisées, le lecteur de cartes se met par défaut en mode verrouillé (« lock »). Votre secteur reste protégé. Si l'immeuble a une génératrice, le lecteur de cartes devrait fonctionner normalement.

10. Que se passe-t-il si quelqu'un oublie sa carte d'accès? Cette personne peut-elle entrer?

Cette personne peut appeler le Service de sécurité au 398-4556. Le Service de sécurité vérifiera ses papiers d'identité. Si elle peut produire une carte d'identification avec photo, un agent de sécurité sera envoyé pour lui ouvrir la porte, à condition que les protocoles de sécurité de votre immeuble ou secteur le permettent.

11. Que dois-je faire si le lecteur de cartes ne fonctionne pas, ou ne lit pas ma carte alors qu'il le devrait?

Envoyez un courriel à campus.security@mcgill.ca ou appelez au 398-4556. Quelqu'un examinera le problème avec vous pour le régler.

12. Que dois-je faire si ma carte de proximité ne fonctionne pas?

Il peut y avoir plusieurs raisons. Vérifiez d'abord auprès du gestionnaire d'accès pour savoir si vos privilèges d'accès sont encore valides. S'ils le sont, envoyez un courriel à campus.security@mcgill.ca ou appelez au 398-4556. Quelqu'un examinera le problème avec vous pour le régler.

FAQ – Systèmes anti-intrusion et composantes

1. Pourquoi et où doit-on installer un système d'alarme anti-intrusion?

Les systèmes d'alarme anti-intrusion servent à protéger l'intérieur des immeubles, bureaux, laboratoires et autres secteurs contenant des biens de grande valeur.

2. Quels dispositifs font partie d'un système d'alarme anti-intrusion?

L'inspection de sécurité déterminera les composantes requises. Le Service de sécurité autorise l'installation d'un système anti-intrusion uniquement si le périmètre entier d'un secteur est protégé. Par exemple, les contacts de porte ne protègent qu'une porte du périmètre d'un secteur, et non l'intérieur d'une pièce. S'il n'y a que des contacts de porte, un voleur peut entrer par une fenêtre et voler vos objets de valeur sans que le Service de sécurité ne reçoive une alarme.

3. Ai-je vraiment besoin d'une sirène?

Oui, les sirènes sont généralement un moyen efficace de dissuasion contre le vol et elles avertissent les gens aux alentours qu'il se passe quelque chose. La décision de ne pas installer une sirène est prise au cas par cas.

4. Où peut-on trouver plus d'information au sujet de l'installation d'un système d'alarme anti-intrusion?

Veuillez consulter l'article 1891 de la Base de connaissances TI à http://www.mcgill.ca/it/.

5. Quel sera le coût?

Le coût sera déterminé par les Services de réseaux et communications après l'inspection de sécurité. On peut obtenir une approximation du coût en consultant l'article 1865 de la Base de connaissances TI à http://www.mcgill.ca/it/.

6. Puis-je encore utiliser les clés pour ouvrir la porte? Faut-il se procurer de nouvelles clés?

Si le système comprend un lecteur de cartes, toutes les portes du périmètre auront une nouvelle serrure utilisable uniquement par le Service de sécurité. S'il n'y a pas de lecteur de cartes avec votre système, vous utiliserez encore les clés. Les contacts de porte n'ont rien à voir avec le mécanisme de verrouillage.

7. Que se passe-t-il en cas de panne de courant? Mon système d'alarme anti-intrusion peut-il fonctionner?

Oui, il peut fonctionner. Le système d'alarme anti-intrusion est muni de piles de secours qui permettent au système de fonctionner un certain nombre d'heures. Si l'immeuble a une génératrice et que le système d'alarme anti-intrusion y est connecté, le système devrait fonctionner normalement.

8. Que se passe-t-il si quelqu'un oublie son code d'accès? Cette personne peut-elle entrer de toute façon?

Non. Le Service de sécurité n'a aucun moyen de vérifier les papiers d'identité d'une personne pour le système d'alarme anti-intrusion sauf pour les abonnés inscrits. Les abonnés ont la responsabilité de donner les codes d'accès à tous les utilisateurs qui ont l'autorisation d'accéder à leur secteur durant les heures de fermeture. Les utilisateurs ont la responsabilité de mémoriser leur code d'accès ou de l'avoir avec eux.

9. Que dois-je faire si je veux changer le code d'accès?

Au cours de l'installation, le Service de sécurité donne une formation à l'abonné sur la façon d'assigner, de retirer et de changer un code d'accès. Les abonnés recevront aussi un manuel d'utilisateur pour leur système.

10. Que dois-je faire si le système anti-intrusion ne fonctionne pas, ou s'il ne lit pas mon code d'accès?

Envoyez un courriel à campus.security@mcgill.ca ou appelez au 398-4556. Quelqu'un examinera le problème avec vous pour le régler.

FAQ - Languettes d'ordinateur personnel et de podium

1. Pourquoi installer des languettes d'ordinateur personnel ou de podium?

Dans une pièce contenant un grand nombre d'ordinateurs, il doit y avoir des languettes pour les protéger contre le vol. Même dans les petits bureaux avec un seul ordinateur, on peut installer une languette de protection si la valeur du matériel et des données le justifie. Les languettes servent aussi à protéger les rétroprojecteurs et les écrans plats de télévision.

2. Où peut-on trouver plus d'information au sujet de l'installation de languettes d'ordinateur personnel ou de podium?

Veuillez consulter l'article 1891 de la Base de connaissances TI à http://www.mcgill.ca/it/.

3. Quel sera le coût?

Le coût sera déterminé par les Services de réseaux et communications après l'inspection de sécurité. On peut obtenir une approximation du coût en consultant l'article 1865 de la Base de connaissances TI à http://www.mcgill.ca/it/.

4. Y a-t-il une limite au nombre de languettes d'ordinateur personnel ou de podium que l'on peut commander à la fois?

Non. Vous pouvez en commander autant qu'il vous faut. Veuillez indiquer le nombre de dispositifs requis sur le formulaire de demande.

5. À quoi peut-on attacher les languettes d'ordinateur personnel ou de podium?

Elles peuvent être attachées aux tours d'ordinateur, aux écrans et aux imprimantes. Elles peuvent aussi servir à protéger divers appareils audiovisuels. Veuillez indiquer dans le formulaire de demande à quels dispositifs seront attachées les languettes.

6. Y a-t-il une procédure spéciale pour pourvoir une pièce entière (comme un nouveau laboratoire d'informatique) de languettes d'ordinateur personnel?

Lorsque vous remplissez le formulaire, indiquez le type de local où vous désirez installer les languettes d'ordinateur personnel. Après avoir inspecté les lieux, le Service de sécurité recommandera toute procédure spéciale ou matériel supplémentaire requis (comme une caméra de surveillance ou un lecteur de cartes).

7. L'installation se fait-elle durant le jour ou la nuit? Pourrais-je utiliser mon ordinateur durant l'installation?

L'installation se fait durant les heures d'ouverture et n'affecte pas votre capacité d'utiliser votre ordinateur.

8. Vais-je entendre cette alarme?

Oui, elle résonne fortement. Bien que cela cause parfois des inconvénients, c'est pour votre sécurité, car la sirène a un effet dissuasif sur un voleur potentiel. Par conséquent, si vous savez à l'avance qu'une languette de sécurité sera déconnectée (par exemple pour déplacer l'ordinateur), communiquez avec le Service de sécurité pour masquer l'alarme, ou désarmez-la vous-même.

9. Quelle est l'intervention habituelle en réponse à une alarme?

Veuillez consulter le *Protocole de surveillance des alarmes de sécurité*.

10. Les languettes d'ordinateur sont-elles toujours efficaces contre le vol? Que puis-je faire de plus pour protéger mes données?

Aucun dispositif de sécurité n'est efficace à 100 % et les languettes de sécurité doivent toujours être utilisées conjointement avec d'autres mesures de sécurité pour augmenter leur efficacité. Le Service de sécurité recommande fortement de faire une copie de sauvegarde de toutes les données importantes ou de les sauvegarder sur un serveur.

11. Que se passe-t-il si un voleur coupe les fils? Est-ce qu'une alarme se déclenche?

Oui. Tout ce qui coupe le contact entre la languette de sécurité et l'ordinateur personnel déclenche une alarme.

12. Puis-je enlever la languette de sécurité si je n'en veux plus?

Oui, on peut l'enlever sans endommager l'appareil ni laisser de marques.

FAQ – Caméras de sécurité

1. Quelle est la fonction des caméras de sécurité? Où devrais-je en installer une?

Une caméra de sécurité est un moyen de dissuasion supplémentaire pour protéger vos biens et votre lieu de travail contre le vol. C'est aussi un moyen d'obtenir de l'information sur les intrus potentiels. Une caméra peut être installée à tout endroit où il y a des biens vulnérables, ou à des postes de contrôle d'accès.

2. Où peut-on trouver plus d'information au sujet de l'installation de caméras de sécurité?

Veuillez consulter l'article 1891 de la Base de connaissances TI à http://www.mcgill.ca/it/. Veuillez aussi consulter le *Protocole d'utilisation des caméras en circuit fermé*.

3. Quel sera le coût?

Le coût sera déterminé par les Services de réseaux et communications après l'inspection de sécurité. On peut obtenir une approximation du coût en consultant l'article 1865 de la Base de connaissances TI à http://www.mcgill.ca/it/.

4. Puis-je utiliser des caméras pour surveiller mes employés?

Non. Les caméras de sécurité doivent être utilisées pour des besoins légitimes en matière de sécurité. Les caméras peuvent être installées pour surveiller des lieux de travail où on a identifié des risques, comme par exemple les comptoirs de service de première ligne, les endroits où on manipule de l'argent comptant, etc. Pour une liste d'endroits où on peut installer une caméra de surveillance, veuillez consulter le *Protocole d'utilisation des caméras en circuit fermé*.

5. Qu'en est-il du droit à la vie privée?

Généralement, dans un lieu de travail, il n'y a pas d'attente raisonnable en matière de protection de la vie privée. Toutefois, dans les bureaux privés, les vestiaires et les salles de toilettes, la surveillance vidéo est presque toujours interdite parce qu'il y a une attente raisonnable en matière de protection de la vie privée dans ces endroits.

6. Si j'installe une caméra, puis-je avoir accès aux images en direct et images enregistrées?

Veuillez consulter le Protocole d'utilisation des caméras en circuit fermé pour savoir où les caméras sont permises. Il y a des restrictions sévères.

7. Pourquoi l'accès aux images en direct et enregistrées est-il si restreint si je paye pour la caméra?

Sans égard à l'attente restreinte en matière de protection de la vie privée dans un lieu public ou un lieu de travail, l'utilisation des caméras en circuit fermé est toujours règlementée par la loi. L'Université a confié au Service de sécurité le mandat de faire en sorte que la surveillance par caméra se fasse en conformité avec toutes les lois fédérales et provinciales et en harmonie avec les valeurs de l'Université.

FAQ – Alarmes anti-hold-up et alarmes de panique

1. À quoi servent les alarmes anti-hold-up et alarmes de panique? Où faut-il les installer?

Une alarme anti-hold-up signifie une chose : un hold-up est en cours. Le Service de sécurité intervient en appelant immédiatement le 911. Les alarmes anti-hold-up doivent être installées uniquement là où on manipule de l'argent. Les alarmes de panique servent à toutes les autres urgences. Leur utilisation et emplacement dépend de la situation dans votre secteur, mais elles sont généralement utilisées et placées dans les aires d'accueil et les points de service à la clientèle.

2. Où peut-on trouver plus d'information au sujet de ces alarmes?

Veuillez consulter l'article 1891 de la Base de connaissances TI à http://www.mcgill.ca/it/.

3. Quel sera le coût?

Le coût sera déterminé par les Services de réseaux et communications après l'inspection de sécurité. On peut obtenir une approximation du coût en consultant l'article 1865 de la Base de connaissances TI à http://www.mcgill.ca/it/.

4. Où l'alarme sonne-t-elle?

Les alarmes anti-hold-up sonnent au Centre opérationnel du Service de sécurité mais ne se font pas entendre sur les lieux. Selon l'endroit où elle se trouve, une alarme de panique peut sonner sur place s'il est préférable de demander l'aide des gens du bureau, ou être silencieuse s'il vaut mieux obtenir l'intervention du Service de sécurité.

5. Que se passe-t-il si quelqu'un appuie sur un bouton de panique par erreur?

Veuillez appeler immédiatement le Service de sécurité pour annuler l'alarme. Donnez votre mot de passe personnel pour confirmer votre identité auprès de notre répartiteur.

6. Pourquoi le Service de sécurité insiste-t-il pour l'installation d'une caméra de surveillance avec l'alarme anti-hold-up ou l'alarme de panique?

Il en va de la sécurité des intervenants qui autrement ne sauraient à quels risques ils s'exposent.