Security Device Installation Protocol
# TABLE OF CONTENTS

1.0 PURPOSE ......................................................................................... Page 1

2.0 SCOPE .......................................................................................... Page 1

3.0 DEFINITIONS .................................................................................. Page 1

4.0 PROTOCOL

4.1 General .......................................................................................... Page 4
4.2 Requisition Process ........................................................................ Page 5
4.3 Card Readers .................................................................................. Page 5
4.4 Intrusion Systems and Components ............................................... Page 6
4.5 AV Tabs ......................................................................................... Page 7
4.6 Video Cameras .............................................................................. Page 7
4.7 Panic Alarms and Hold-up alarms ................................................ Page 8
4.8 Service Support, Repair and Maintenance .................................... Page 8
4.9 Decommissioning and Removal ................................................... Page 9

5.0 RESPONSIBILITIES

5.1 Security Services ........................................................................... Page 9
5.2 NCS ............................................................................................ Page 10
5.3 FOD ............................................................................................ Page 10

6.0 ANNEXES

Annex A: FAQ – Card Readers .......................................................... Page 12
Annex B: FAQ – Intrusion Systems and Components .......................... Page 15
Annex C: FAQ – AV Tabs ................................................................. Page 17
Annex D: FAQ – Security Cameras .................................................. Page 19
Annex E: FAQ – Panic and Hold-up Alarms ...................................... Page 21
1.0 PURPOSE

1.1 McGill University Security Services administers the University’s central security system, which includes overseeing the alarm monitoring operation, card access control system, and the security camera network. In order for the system to be effective and efficient, security devices must be installed and utilized in accordance with established standards and best practices.

1.2 Asset protection must be cost-effective. There is a belief that human safety and material integrity improve as greater numbers of security systems and devices are installed. This is false, and a security system or device is only effective if it is used properly. A security device should never be used as a substitute for individual care and caution.

1.3 The protocol outlined in this document has two (2) goals:

1.3.1 The establishment of a process and consistent standards regulating the selection, purchase, installation, and operation of security devices that promote and maintain a safe and secure environment at McGill University.

1.3.2 The reduction of the incidence of false alarms caused by installation issues. False alarms degrade the system’s effectiveness and increase the operating costs.

2.0 SCOPE

2.1 This protocol applies to all current and future University sites under the operational jurisdiction of Security Services, including new construction and capital improvement projects. It also applies to any environmental control alarm to be monitored by Security Services.

2.2 It applies to any space leased by the University where the security device will be monitored by Security Services.

2.3 This protocol does not apply to fire protection systems as they are managed by the Fire Prevention Office.

3.0 DEFINITIONS

3.1 **Access Control System**: a device or electronic system restricting physical access and entry to authorized persons. This type of system is used in areas that have a large number of authorized users entering at various times of the day or night. An access control system usually replaces a traditional key system.
3.2 **Area Access Manager (AAM):** a designated person within a department or faculty responsible for managing its card reader(s) by assigning and removing cardholder access to their areas and establishing and modifying card reader settings. AAMs receive specific training from Security Services. An AAM is distinct from a <subscriber> although the same person can assume both roles.

3.3 **AV Tab (Formerly Personal Computer (PC) and Podium Tab):** a type of sensor consisting of a fibre-optic loop forming a circuit generally used to secure expensive pieces of equipment within an alarmed area. The loop is secured to the equipment. When the equipment is removed, the circuit is broken, and the alarm activates.

3.4 **Card Reader:** is an electronic device that can read a specific identification badge such as a proximity card, verify the access rights associated with that badge and unlock predetermined doors or operate elevators should the access rights be valid. It has dual-function capabilities. See also <Dual-function System>.

3.5 **Door/Window Contact:** a sensor installed within the frame or on the surface of a door or window. The sensor is part of the intrusion alarm system. It detects the opening and closing of the door or window and will signal an alarm if an unauthorized entry or exit is made.

3.6 **Dual-function System:** an electronic system such as a card reader that operates both as an access control and intrusion alarm system.

3.7 **Enhanced Call Verification:** a procedure whereby the Security Operations Centre makes a minimum of two telephone calls to two pre-determined contact persons prior to dispatching a security patrol to investigate the alarm. If a contact person answers, indicates an error, and confirms his/her identity with a password, the alarm is resolved and no security patrol is dispatched.

3.8 **Exit Detection Device:** a motion sensor used to permit egress through an alarmed door without setting off the alarm.

3.9 **Glass Break Detector:** a type of sensor designed to monitor the alarmed area for the specific sound of breaking glass.

3.10 **Hold-up Alarm:** a button alarm activated when a hold-up (robbery) or attempted hold-up takes place. The hold-up alarm is reserved for use at cashiering points or other areas where money is handled. Hold-up alarms summon immediate response by police. See also <Panic Alarm>.

3.11 **IACLEA:** the International Association of Campus Law Enforcement Administrators.
3.12 **Intrusion Alarm System**: uses motion sensors, door/window contacts, and other devices to detect the presence, entry or attempted entry of an intruder into the supervised area. It sends a signal to the Security Operations Centre when such an event occurs.

3.13 **Keypad**: the device into which the user enters a numeric code, key, or scans a proximity device, such as a card or fob, to arm (turn the alarm "on") or disarm (turn the alarm "off") the intrusion alarm system.

3.14 **Motion Sensor**: a device monitoring movement within an alarmed area. The motion sensor connects to the intrusion alarm panel and it is part of the intrusion alarm system.

3.15 **Panic Alarm**: a panic button alarm is used in locations where life threatening, medical aid or other situations requiring an immediate emergency response may arise. Panic alarms are usually installed at frontline customer service points, but portable alarms are also available. See also <Hold-up Alarm> for cash disbursement points.

3.16 **Partition**: a group of zones within a larger intrusion alarm system that permits a number of areas to be armed or disarmed independently from a single intrusion alarm panel. Due to repeated instances of user error, Security Services no longer permits new installations with partitions.

3.17 **Password**: a confidential alphanumeric code used to authenticate users when they call Security Services.

3.18 **Proximity Card**: a generic name for contactless integrated circuit devices used for security access. McGill University uses three types of proximity cards: (1) the McGill staff and student card with photo; (2) a blank proximity card for temporary employees and visitors; and (3) the McGill Service Provider ID card for employees of contracted firms working at McGill.

3.19 **Requestor**: someone who requests a security device. A requestor may be the end user or someone representing the end user (e.g. project manager, faculty or department administrator, or building director).

3.20 **Security Operations Centre**: serves as the main alarm monitoring station for the University. There is one for each of the Downtown and Macdonald campuses.

3.21 **Subscriber**: a faculty, department, or outside agency at McGill University operating a security device; or the designated person responsible for managing a security device. A subscriber who manages a card reader is referred to as an Area Access Manager.

3.22 **Users**: are members of the McGill community who use, work or study in, or have authorized access to the area protected by the security device installed by the owning faculty or department.
3.23 **Zone**: a specific area within the alarmed area monitored by the intrusion alarm system. Current standards allow for only one sensor device per zone for the safety of the responders and to improve diagnostic capability. This restriction does not apply to AV Tabs.

### 4.0 PROTOCOL

#### 4.1 General

4.1.1 All security devices installed on McGill University controlled sites require the approval of Security Services.

4.1.2 Where applicable, all security devices installed in a McGill building must have the approval of the building director.

4.1.3 Where it is not covered by the lease agreement, all security devices installed in a commercially rented space must have the approval of the landlord.

4.1.4 No security device on a McGill University controlled site shall be removed without the approval of Security Services.

4.1.5 All security devices on a McGill University controlled site will be installed by Network and Communication Services (NCS) or a qualified contractor approved by NCS.

4.1.6 To facilitate alarm investigations, room numbers to all areas containing a security device must be visibly displayed at all times.

4.1.7 If a space containing security devices is going to be repurposed, Security Services must be advised so that a proper evaluation can be made to determine if the current security devices will support the new space. Failure to do so may result in a cessation of service support and/or alarm monitoring services.

4.1.8 Security devices in place that are no longer used must be decommission by NCS at the expense of the device owner.

4.1.9 Access to all areas containing security devices or alarm equipment must be provided to Security Services by the subscriber so that responding security personnel can investigate any possible crimes in progress. Where the area is restricted for safety reasons, an alternative response protocol must be established.
4.2 Requisition Process

4.2.1 Requestors who wish to install a security device may contact Security Services directly at systems.security@mcgill.ca.

4.2.2 Security Services will perform an on-site assessment to determine the requestor’s security needs and propose the most effective solution. The assessment will evaluate the security of the area, personnel safety, alarm responder safety, and current alarm technologies. As a result, Security Services may actually recommend a different solution than the one originally requested.

4.2.3 The process of the on-site assessment may include consultation with Network and Communication Services (NCS), Facilities Operations and Development (FOD), and/or the Fire Prevention Office (FPO). The on-site assessment and scope of work draft will take approximately two weeks to perform.

4.2.4 Security Services will then ask for a budget amount from NCS and FOD to install the requested device. Security Service will be responsible for including estimates from NCS and FOD in the Security Device Request form. The length of this process is variable, especially if custom installations are required. Security Services will then forward the budgetary amount to the requestor for approval.

4.2.5 If the requestor approves the anticipated cost, a FOAPAL or Client number will be required for billing. The length of the installation process is variable. Special hardware purchases may be required, and their acquisition may delay the process.

4.2.6 For major renovation and construction projects, Security Services requires sixty (60) days advance notice prior to the anticipated delivery date.

4.2.7 As part of the installation process, the requestor must designate a minimum of two (2) subscribers to be trained by Security Services and be responsible for the device.

4.2.8 After the security device is physically installed, Security Services will complete the configuration, perform an inspection and advise the subscriber when the device is ready to go “live”.

4.3 Card Readers

4.3.1 A card reader is primarily an access control device. Requestors seeking a security device to protect valuable property will be urged to acquire an intrusion alarm system controlled by a keypad that will be monitored 24/7 (when armed).
4.3.2 There are three different types of card reader installations at McGill University, each with a different level of service:

i. card reader with alarm monitoring;
ii. card reader for access control only; and
iii. card reader for key use only.

Refer to Annex A for more details about each type of installation.

4.3.3 The door on which the card reader is to be installed has to meet the following requirements:

i. the door must be in good condition and suited for a card reader system;
ii. the door must have a door closer (alarm monitoring feature only);
iii. the door must have an exit detection device (alarm monitoring feature only);
iv. electric strikes should be “fail-secure”, so that when exit device is activated, it only bypasses the door contact, but does not unlock the door; and
v. the door must have a Medeco cylinder pinned on a restricted keyway only available to Security Services so that users cannot bypass the card reader with a key. This does not apply to card readers “for key use only.”

4.3.4 If there are other doors that provide access to the space, they will require security devices and door hardware changes, depending on the type of card installation requested. See Annex A for details.

4.3.5 Where applicable, Security Services will monitor card readers for alarms in accordance with its Security Alarm Monitoring Protocol, a copy will be provided to the client as part of the installation process.

4.4 Intrusion Systems and Components

4.4.1 An area where an intrusion alarm system is requested for must meet the following conditions:

i. doors must be in good condition and suited for contacts or other devices;
ii. windows must be in good condition and suited for contacts or glass-break detectors; and
iii. motion sensors must not be obstructed by furniture or light fixtures.

4.4.2 The following standards will apply to all intrusion alarm systems installed at McGill University:

i. keypads must be installed at every entrance used to enter an alarmed area;
ii. each alarm type (intrusion, unknown trouble, tamper, low battery) must report on a separate zone;
iii. glass break detectors must be linked to an intrusion system with keypad;
iv. each intrusion sensor must report on a separate zone unless otherwise approved by Security Services, exceptions will only be made for devices of the same type in the same room;
v. zones must be clearly labeled on the keypad;
vi. an audible siren sounding for at least one minute is required for all intrusion detection systems;
vii. the keypad must emit an audible sound for the exit delay alerting the user that the exit delay cycle has started; and
viii. the keypad must emit an audible sound for an exit error fault alerting the user when an error has been made when arming the alarm or leaving the alarmed area.

4.4.3 Security Services will monitor intrusion alarm systems in accordance with its Security Alarm Monitoring Protocol, a copy will be provided to the subscriber as part of the installation process.

4.5 **AV Tabs (Formerly Personal Computer (PC) and Podium Tabs)**

4.5.1 AV tab installations should always be part of a broader security system that also includes locking devices, card readers, security cameras; etc.

4.5.2 AV tab installations must be accompanied by a siren.

4.5.3 Any room with more than five (5) AV tabs must have an alarm panel to be managed by the subscriber.

4.5.4 Note that all television flat screen monitors installed by NCS Multimedia Services are affixed automatically with an AV tab.

4.6 **Video Cameras**

4.6.1 Camera installations and access to live and recorded images are governed by the CCTV Protocol.

4.6.2 The location for outdoor camera installations for the Downtown Campus needs to be approved by Design Services.
4.7 Panic Alarms and Hold-up Alarms

4.7.1 Panic alarms and hold-up alarms should never be used as the sole solution to a security risk. They must always be employed as a complement to other security measures to address that risk.

4.7.2 Users of panic alarms and hold-up alarms are strongly encouraged to take the De-escalating Potentially Violent Situations training provided by Security Services.

4.7.3 All users of panic alarms must have authentication passwords to call Security Services in the event of a false alarm.

4.7.4 The subscriber requesting a panic alarm must also install a camera or provide a minimum of two contact numbers on site other than the panic alarm user whereby the Security Operations Centre can confirm the nature of the emergency while the security patrol is on route.

4.7.5 If the panic alarm is not monitored by Security Services and is designed to summon local office assistance only, it need not meet the above-mentioned requirements.

4.7.6 In accordance with IACLEA standards, all panic alarms monitored by Security Services must be tested quarterly.

4.7.7 In accordance with IACLEA standards, Security Services will re-evaluate the security situation that prompted the installation of the panic button every two years. If the security needs are no longer the same, the panic button may be decommissioned.

4.7.8 A hold-up alarm installation is reserved only for areas where money is handled and must be accompanied by a camera installation. The activation of a hold-up alarm results in an immediate response from police.

4.7.9 Subscribers will be held accountable for any fines resulting from false reports to 911 following hold-up alarms.

4.8 Service Support, Repair and Maintenance

4.8.1 The subscriber’s responsibilities and the client support Security Services undertakes to provide after the installation are outlined in the Service Level Commitment for Security Devices, a copy will be provided to the subscriber as part of the installation process.
4.8.2 All new installations performed by NCS or its hired contractors carry a twelve month warranty on parts and labour from the date the installation is completed. Beyond this warranty period, repairs and replacement parts are at the charge of the owners of the peripheral components.

4.8.3 Security Services will submit work orders with NCS or FOD on behalf of the subscriber when alarm responders come upon incidents of equipment failure. Billable repairs will not be executed without client approval.

4.9 Decommissioning and Removal

4.9.1 Subscribers who wish to decommission their security device must submit their request to Security Services. The process followed will be similar to the requisition process.

4.9.2 When a unit relocates and departs from a leased commercial space, and there is not another McGill unit moving in, the decommissioning and removal of security devices, if required by the landlord, must be part of the project, along with any necessary repairs to walls, doors, etc. This work shall be coordinated with the landlord’s representative.

4.9.3 When a unit relocates and departs from a campus space and does not want to transfer the security devices to its new space:
   
   i. the decommissioning and removal of security devices must be part of the project unless there is a firm commitment to use the devices from the incoming occupant; but
   
   ii. if incoming occupant is not yet identified, the project must make a provision to remove the devices even if they stay until a final decision is rendered by the new occupant

4.9.4 The stipulation above does apply to card readers. At the request of FOD Project Management, card readers will no longer be transferable with unit relocations from a campus space because there is no cost saving. Outgoing units will be provided with funding for new card readers.

5.0 RESPONSIBILITIES

5.1 Security Services provides consulting expertise on loss prevention and crime risk management. We develop and implement standards concerning security devices deployed on campus, approve their installation and removal, and are responsible for the management and operation of the central alarm monitoring system.
5.2 NCS is responsible for the deployment and maintenance of security device installations that are monitored by the University’s central alarm monitoring station. It is also responsible for the purchase of all security devices requested and approved based on established standards.

5.3 FOD is responsible for the deployment and maintenance of security device hardware and peripherals for installations that are monitored by the University’s central alarm monitoring station. It is also responsible for the purchase of all hardware requested and approved based on established standards.

6.0 ANNEXES

Annex A: FAQ – Card Readers
Annex B: FAQ – Intrusion Systems and Components
Annex C: FAQ – PC and Podium Tabs
Annex D: FAQ – Security Cameras
Annex E: FAQ – Panic and Hold-up Alarms

7.0 REVISION HISTORY

Amended:
20 December 2018 – modified name of PC Tabs to AV Tabs to reflect new naming convention. Modified instruction for the requisition process to send email to systems.security@mcgill.ca (form decommissioned). Updated training provided by Security to De-Escalating Potentially Violent Situations. Updated responses in FAQ section.

Amended:
13 November 2015 – Added a clause reinforcing that it is the device owner’s responsibility to remove security devices no longer in use; modified the term "price quote" to “budget estimate” to reflect the pricing process change by NCS; removed the specific timeline delivery of the budget estimate because it is not within our control; removed the citation whereby PC Tabs are automatically installed on overhead projectors.

Amended:
30 April 2014 – Modified the clause regarding environmental control alarms where they are now subject to our approval for installation if they are monitored by us regardless of the monitoring system; added a clause to address spaces that are repurposed; modified the section and FAQ on card readers to account for the different types of installations offered; modified the section on panic buttons to incorporate the IACLEA standard; added more information to the FAQ on security cameras.
Amended:
21 June 2012 – Modified the section on security cameras to address outdoor installations.

Amended:
18 November 2011 – Consolidated all information into one document; added a section of definitions, stipulated the standards and requirements for each type of device.

Baseline Document:
20 October 2006 – each security device had its individual document.
FAQ – Card Reader

1. What type of space can have a card reader?
   Any room, lab or building can have a card reader. In short, a card reader can go any place where an area needs to be secured. Card readers replace key systems, which can be easily duplicated or lost and create a security risk. Card readers use existing McGill ID badges and allow the administrators to award and revoke access from users at any time, and also to determine area access at particular times. Card readers are not ideal for spaces which have highly variable opening hours.

2. Is a card reader always the best access control solution?
   No. The use of card readers has its limits. Make sure the Security Services consultant understands how you intend to use the space, especially the scheduled use of it. The card reader and the services we offer with it may not have the flexibility to support your need.

3. How can the card reader be used?
   Security Services offers three different levels of use.
   (1) Card reader with alarm monitoring – this type of installation is equipped to detect door held open and door forced open alarms. Any other door that provides access to the space will have to be modified also. Moreover, the alarm monitoring is limited to what is provided in the Security Alarm Monitoring Protocol. This would not be a practical application for areas that are occupied at all hours of the day.
   (2) Card reader for access control only – this type of card reader installation is not equipped or programmed to detect door held open or door forced open alarms. Any other door that provides access to the space will have to be modified also to ensure effective access control.
   (3) Card reader for key use only – this is the least expensive option because the door hardware modifications to other doors providing access to the space are not required. The card reader replaces the key lock on the particular door. Other doors to the space need not be modified but card reader reports for this type of installation will not be provided. Note that this option is only available to areas where there are multiple doors to the space. If the space contains only one access door, the standards are the same as for a card reader for access control only.
4. **Where can I find more information about card reader installations?**


5. **What will the cost be?**

   The cost will be determined by NCS and FOD after the security review. A rough idea of the cost can be obtained by consulting Article 1865 of the IT Knowledge Base at [http://www.mcgill.ca/it/](http://www.mcgill.ca/it/). Note that the door hardware requirements will be the variable factor for cost and delivery time. For example, some doors may not be suitable for a card reader and may need to be replaced. Fire-rated doors require a special installation that is more expensive.

6. **Will I be able to work in the area while it's being installed?**

   Yes.

7. **Does having a card reader mean there are no keys involved at all?**

   Yes. The locks will be changed so that your keys no longer work. All individuals with keys need to receive access on their ID badges. Only Security Services will have the override key for emergency purposes. This does not apply to card readers “for key use only.”

8. **Does a card reader eliminate the need for other security devices inside the protected area?**

   A card reader is used primarily for access control. If you wish to protect the property inside, the security survey will recommend the options available.

9. **Does Security Services monitor card readers for alarms?**

   Please consult the [Security Alarm Monitoring Protocol](#).

10. **Can I request a report to review who accessed my area?**

    For some restricted areas, especially where government regulatory compliance is in force, reader reports can be provided on a regular basis. For all other areas, requests for reader reports must be accompanied by the reason for the report. Requestors should include as many relevant details so that we can approve the request without delay. This is to prevent possible misuse of a security device. For example, reader report requests will not be approved if the requestor intends to use the report to confirm payroll hours or work attendance. This requires approval from Human Resources. Similarly, reader report
requests will not be approved if the requestor intends to use it for a criminal investigation as this is the purview of Security Services.

11. **What happens if the power goes out? Will my card reader still work?**

   Yes, it will. The card readers all have backup batteries which will operate the card reader for a number of hours depending on how many security devices and panels you have in your building. When the back-up batteries fail, the card reader will default into <lock> mode. Your area will remain secure. If the building has a generator, the card reader should work as per normal.

12. **What happens if someone forgets their access card? Can they still get in?**

   They should contact the area supervisor or Area Access Manager to arrange a temporary access solution.

13. **What should I do if the card reader is malfunctioning, or doesn’t read my card when it should?**

   E-mail systems.security@mcgill.ca or call 398-4562. Someone will investigate or troubleshoot the matter with you.

14. **What should I do if the proximity card is malfunctioning?**

   There may be a number of reasons for this. First, verify with the Area Access Manager to determine if your access privileges are still valid. If they are, e-mail systems.security@mcgill.ca or call 398-4562. Someone will investigate or troubleshoot the matter with you.
FAQ – Intrusion Systems and Components

1. **Why and where should I get an intrusion alarm system?**
   Intrusion alarm systems are used to protect the interior of buildings, offices, labs and other areas where there are valuable assets.

2. **What devices come with an intrusion alarm system?**
   The components required will be determined by the security survey. Security Services will not authorize the installation of an intrusion system unless the entire perimeter of an area is protected. For example, door contacts only protect the perimeter door of an area, not the inside of a room. With door contacts alone, a thief could break in through a window and steal your valuables without Security Services receiving an alarm.

3. **Do I really need a siren?**
   Yes, Sirens are generally an effective deterrent to theft and lets others nearby know something is going on. Exceptions to installing a siren will be made on a case-by-case basis only.

4. **Where can I find more information about intrusion alarm systems?**

5. **What will the cost be?**
   The cost will be determined by NCS and FOD after the security assessment. A rough idea of the cost can be obtained by consulting Article 1865 of the IT Knowledge Base at [http://www.mcgill.ca/it/](http://www.mcgill.ca/it/). This cost does not include any required hardware modifications or peripherals.

6. **Do I still use keys to open the door? Will I need new keys?**
   If the system comes with a card reader, all perimeter doors would be rekeyed to a restricted keyway available to Security Services only. If there is no card reader with this system, you would still use keys. Door contacts have no effect on the locking mechanism.
7. **What happens if the power goes out? Will my intrusion alarm system still work?**

   Yes, it will. The intrusion alarm systems come with a backup battery which will operate the system for a number of hours. If your building has a generator and intrusion alarm system is a device connected to it, the system will work as per normal.

8. **What happens if someone forgets their access code? Can they still get in?**

   No. Security Services has no way to verify a person’s credentials for intrusion alarm systems except for registered subscribers. Subscribers are responsible for providing access codes to all users they authorize access to their area during silent hours. Users are responsible to memorize or have their access code on their person.

9. **What do I do if I wish to change the access code?**

   As part of the installation process, Security Services will train the subscriber on how to assign, remove, and change an access code. Subscribers will also be provided with a user manual for their system.

10. **What should I do if the intrusion system is malfunctioning, or doesn’t read my access code when it should?**

    E-mail systems.security@mcgill.ca or call 398-4562. Someone will investigate or troubleshoot the matter with you.
FAQ – AV Tabs (Formerly Personal Computer (PC) and Podium Tabs)

1. **Why should I get an AV Tab?**

   Any valuable and fixed equipment should have AV Tabs to guard against theft, depending on the value of the assets, both physical and data-based. AV Tabs are primarily used to protect public displays and valuable AV equipment but may have other applications. These security tabs should always be an accompaniment to a locking device.

2. **Where can I find more information about AV Tabs?**


3. **What will the cost be?**

   The cost will be determined by NCS after the security assessment. A rough idea of the cost can be obtained by consulting Article 1865 of the IT Knowledge Base at [http://www.mcgill.ca/it/](http://www.mcgill.ca/it/)

4. **Is there a limit to how many AV Tabs can I order at once?**

   No. You may order as many as you need.

5. **To what can I attach an AV Tab?**

   They can be attached to valuable equipment that is installed in a fixed location. They can be used to protect a variety of audio-visual equipment. Please indicate what device(s) you want the tab(s) attached to when placing your request.

6. **Is the installation done during the day or night? Will I be able to use my equipment during installation?**

   Installation is performed during business hours and will not affect your ability to use your equipment.
7. **Will I hear this alarm?**

Yes, it will sound loudly. While this may be occasionally inconvenient, it is for your security, as the siren acts an effective deterrent to a potential theft. Therefore, if you know that there is the possibility that the security tab will become disconnected (such as while moving the equipment), contact Security Services to mask the alarm, or disarm it yourself.

8. **What is the typical response to an alarm?**

Please consult [Security Alarm Monitoring Protocol](#).

9. **Do AV Tabs always work as a deterrent to theft? What else can I do to protect my data?**

No security device is 100 percent effective and security tabs should always be used in conjunction with other security measures to increase their effectiveness. Security Services strongly recommends that all important data be backed up or saved on a server.

10. **What happens if a potential thief cuts the wires? Does that trigger an alarm?**

Yes. Anything that causes the security tab to lose communication with the AV equipment will trigger an alarm.

11. **Can the security tab be removed if I no longer want it?**

Yes, it can be taken off without causing damage to the machine or leaving any marks.

12. **Can I install AV Tabs on a computer?**

Generally AV Tabs are no longer installed on computers due to the high volume of nuisance alarms generated. However, there are other options for securing a computer including a physical lock or intrusion system in the area.
FAQ – Security Cameras

1. **What is the purpose of a security camera? Where should I put one?**

   The purpose of a camera is an added deterrent to protect your assets and workspace from theft and to potentially provide information about intruders. A camera can be installed in any location where there are vulnerable assets or access controlling points.

2. **Where can I find more information about security cameras?**


3. **What will the cost be?**

   The cost will be determined by NCS after the security survey. A rough idea of the cost can be obtained by consulting Article 1865 of the IT Knowledge Base at [http://www.mcgill.ca/it/](http://www.mcgill.ca/it/).

4. **Do cameras reduce theft?**

   Video surveillance by itself is not a proven crime deterrent. The ability of camera surveillance to deter crime will vary according to location and the type of crime committed. It should always be used along with other crime reduction measures. Cameras are much more effective where they are employed correctly and in tandem with other security measures.

5. **My staff complains about lunches being stolen from the kitchen refrigerator. Would a camera help?**

   This does not meet the criteria for an approved security camera installation at McGill University. Other measures are available to resolve this issue.

6. **Can our cameras perform like on television police dramas such as CSI?**

   No. Such television shows can create unrealistic expectations when people are victims of real crimes. The actual CCTV technology in a shopping mall, subway station, or university is far less fantastic. If a camera's purpose is to monitor access and egress through a doorway, do not expect it to capture someone stealing a wallet left alone on a table many metres away.
7. **Can I use cameras to monitor my employees?**

   No. Security cameras are to be used for a legitimate safety or security reason. Cameras may be placed to monitor work areas where there is an identified risk such as frontline service counters; cash distribution points, etc. For a list of areas where cameras may be placed, please consult the [CCTV Protocol](#).

8. **What about the right to privacy?**

   Generally, a workplace does not provide a reasonable expectation of privacy. However, private offices, changing rooms and washrooms are almost always off limits for camera surveillance because those are areas where an expectation of privacy exists.

9. **If I install a camera, can I have access to live images and recorded images?**

   Please consult the [CCTV Protocol](#) where this is permitted. There are severe restrictions.

10. **Why is access to live and recorded images so restricted if I am paying for the camera?**

    Regardless of the limited expectation of privacy in a public area or workplace, the use of CCTV is still regulated by law. The University has mandated Security Services to ensure that camera monitoring is conducted in a manner compliant with all existing federal and provincial laws and consistent with the values of the University.
FAQ – Panic and Hold-up Alarms

1. What is the use of a panic or hold-up alarm? Where should I put one?
A hold-up alarm means one thing: that a hold-up is in progress. The response by Security Services will be to call 911 immediately. Hold-up alarms should be used exclusively where money is handled. Panic alarms are for all other emergencies. Their use and location will depend on the situation in your area, but they are generally used and located in reception areas and customer service points. There needs to be a demonstrated need before a panic or hold-up button will be installed.

2. Where can I find more information about these alarms?
Please consult Article 1891 of the IT Knowledge Base at http://www.mcgill.ca/it/.

3. What will the cost be?
The cost will be determined by NCS after the security assessment. A rough idea of the cost can be obtained by consulting Article 1865 of the IT Knowledge Base at http://www.mcgill.ca/it/.

4. Where does the alarm ring?
Hold-up alarms ring at the Security Operations Centre but are silent locally. Depending on your situation, a panic alarm can ring locally if the ideal response is to summon aid from within your office or silently if the ideal response is to have Security Services respond.

5. What happens if the panic button is pressed by mistake?
Please call Security Services immediately to cancel the alarm. Provide your individual password to confirm your identity to our Controller.

6. Why does Security Services insist on a camera installation with a hold-up or panic alarm?
It is for the safety of the responders who would otherwise go in blind at a risk to themselves.