# 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 Alarm Monitoring of Buildings – Perimeter ............................................. Page 5
  4.3 Alarm Monitoring of Buildings – Interior Room or Area ..................... Page 6
  4.4 Alarm Monitoring of Personal Computer and Podium Tabs .............. Page 7
  4.5 Hold-up and Panic Alarms ....................................................................... Page 7
  4.6 Environmental Control Alarms ............................................................... Page 7
  4.7 False Alarms ............................................................................................. Page 8

5.0 Roles and Responsibilities

  5.1 Security Services ....................................................................................... Page 8
  5.2 NCS ........................................................................................................... Page 9
  5.3 Service Level Commitment for Security Devices .................................. Page 9

6.0 Annexes

    Annex A: Alarm Monitoring by Room Type ............................................. Page 10
1.0 PURPOSE

1.1 McGill University Security Services maintains and operates a central security alarm monitoring system at both the Downtown and Macdonald campuses. The purpose of this protocol is to define a standard level of alarm monitoring service that will be provided to McGill alarm system subscribers.

1.2 The protocol outlined in this document has three (3) goals:

   1.2.1 To maintain a sustainable structure that provides an effective means of protection and deterrence against crime.

   1.2.2 To provide operating standards to ensure for the safety of the alarm responders.

   1.2.3 To reduce the incidence of false alarms that waste resources and restrict our ability to respond to legitimate incidents.

2.0 SCOPE

2.1 This protocol applies to all security alarm systems used by University departments or any non-university entity under contract with the University. It also applies to all environmental alarms monitored by Security Services.

2.2 This protocol does not apply to fire protection systems which are monitored by an outside agency.

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 uses entering at various times of the day or night. An access control system usually replaces a traditional key system.

3.2 **Alarm Monitoring Service**: Security Services provides a central station to receive all alarms and will initiate a response in accordance with established protocols. The response will vary in accordance with the type of alarm, the location of the alarm and the time of day.

3.3 **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 the responsibilities for both.

3.4 **Card Only**: a setting on proximity card readers that obliges the user to utilize a proximity card with authorized permissions in order to unlock a door. During this setting, the light on a card reader is red.

3.5 **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>.

3.6 **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.

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

3.8 **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 the contact person answers, indicates an error, and confirms his/her identity with a password, the alarm is resolved and no security patrol is dispatched.

3.9 **Environmental Control Alarm**: an alarm that signals a problem with temperature, water leak, smoke, gas, humidity, or the operating systems that control the desired environment.

3.10 **False Alarm**: a security alarm that was not caused by a criminal act or a threat to safety.

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

3.12 **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. See also <Panic Alarm>.

3.13 **Intrusion Alarm System**: uses motion sensors, door/window contacts, and other devices to detect an unauthorized entry into an alarmed area. It sends a signal to the Security Operations Centre when one occurs.
3.14 **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.

3.15 **Lock or Locked Down**: a setting on proximity card readers that locks the card reader to all users regardless of authorized permissions. During this setting, the light on a card reader is red. Only Security Services has the authority to place a card reader on <Lock> mode.

3.16 **Mask**: a setting whereby the security device remains armed but does not send an intrusion alarm to the Security Operations Centre. See also <Unmask>.

3.17 **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.

3.18 **Operating Hours**: refers to the hours when a building, room, or area is open. Where a building, room, or area is on <card only> 24/7, the default operating hours are defined as 08h00-18h00, the daytime working hours of the majority of employees. Operating hours for major academic buildings are generally 07h00–22h00. Operating hours for smaller academic and office buildings are more circumscribed. See also <Silent Hours>.

3.19 **Panic Alarm**: a panic button alarm 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.

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

3.21 **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.

3.22 **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.

3.23 **Security Operations Centre**: serves as the main alarm monitoring station for the University. There is one for each of the Downtown and Macdonald campuses.
3.24 **Silent Hours**: refers to the time when a building, room or area is closed and access is restricted to authorized users only. Where a building, room, or area is on 24/7, the default silent hours are defined as 18h00-08h00. Silent hours for major academic buildings are generally 22h00-07h00. Silent hours for smaller academic and office buildings are generally more extended. See also <Operating Hours>.

3.25 **Subscriber**: a faculty, department, or outside agency at McGill University operating a security device. A subscriber representative who manages a card reader is referred to as an Area Access Manager.

3.26 **Unlock**: a card reader or electric lock setting that unlocks the door permitting unfettered access; used when the area is open. During this setting, the light on the card reader is green.

3.27 **Unmask**: a setting whereby the system resumes sending intrusion alarms to the Security Operations Centre. See also <Mask>.

3.28 **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.

4.0 **PROTOCOL**

4.1 **General**

4.1.1 Security Services will provide an alarm monitoring and response service to McGill faculties, departments and other units free of charge in accordance with the criteria set out in this protocol.

4.1.2 This service will be provided only for alarm system installations that were approved by Security Services. Alarm monitoring by Security Services begins when the installation is complete and the subscriber has provided Security Services with the necessary information to complete the security device request.

4.1.3 If the room or space monitored by Security Services is remodelled or repurposed, Security Services must be advised prior by the subscriber, faculty or department using that space. Failure to do so may result in the suspension of the alarm monitoring service as it was configured for the original use of the space.

4.1.4 Security Services can only provide limited services to McGill units housed in leased commercial office buildings. The amount of service is determined on a case-by-case basis.
4.1.5 Security Services will not provide an alarm monitoring service to a building or space that has been turned over to a contractor for construction or renovations. Security of the work site becomes the responsibility of the contractor.

4.1.6 Security Services will prioritize its alarm response in the following order:
   (i) alarms protecting people;
   (ii) alarms protecting property; and
   (iii) environmental control alarms.

4.1.6 Depending upon the type of alarm, the zone triggered, number and sequence of zones, time of day, and other factors, the actions that will be initiated by the Security Operations Centre include, but are not limited to:
   (i) alerting 911;
   (ii) alerting a subscriber representative on location during operating hours;
   (iii) alerting a subscriber representative at home during silent hours;
   (iv) alerting a subscriber representative via an automatic email;
   (v) alerting the appropriate maintenance department;
   (vi) verifying the area using video cameras; and/or
   (vii) sending one or more patrollers to investigate.

4.1.7 When a patroller is dispatched to an alarm, the arrival time will depend on different variables such as weather, road and traffic conditions, and the location of the incident in relation to the patroller’s current location. Security Services vehicles are not emergency vehicles. When and where possible, we will arrive within:
   (i) ten (10) minutes for alarms protecting people; and
   (ii) twenty (20) minutes for all other alarms.

4.2 Alarm Monitoring – Building Perimeter

4.2.1 Security Services will monitor all perimeter doors of a building during its silent hours.

4.2.2 Except for certain types of buildings such as libraries and retail stores, Security Services will not monitor perimeter doors when the building is open. The security devices on the doors will be masked.
4.2.3 Where a building is on the setting <card only> 24/7, Security Services will not monitor the perimeter during its operating hours. The security devices on the doors will be masked.

4.2.4 Security Services will not provide an intrusion alarm monitoring service to a building unless all perimeter doors are equipped with a security alarm device. Subscribers who wish to have alarm monitoring service for a card reader door will require that all other perimeter doors be equipped with a door contact as a minimum. Security Services will not endorse partial perimeter coverage.

4.2.5 Subscribers with an intrusion alarm system controlled with a keypad must provide Security Services with two email addresses or two telephone contacts to alert if an alarm is triggered during operating hours. Security Services will not dispatch a patrol during this time. If the alarm is triggered during silent hours, Security Services will dispatch a patrol immediately.

4.3 Alarm Monitoring – Building Interior

4.3.1 Security Services will provide its intrusion alarm monitoring and response service in accordance with the grid found in Annex A. The hours listed are default settings that may be further restricted by Security Services based on the traffic and occupancy rate of the space.

4.3.2 Areas protected by a card reader and associated door/window contacts:
   (i) In general, Security Services will not provide an intrusion alarm monitoring service to areas protected by a card reader and associated door/window contacts when the building is open because the areas are considered “occupied”. The devices will be masked. Exceptions are reserved for areas designated as high risk or where required for reasons of regulatory compliance.
   (ii) For office areas, the default operating hours will apply and no alarm monitoring will be performed between 08h00-18h00.

4.3.3 Areas protected by an intrusion alarm system controlled by a keypad:
   (i) Subscribers must provide Security Services with two contacts to alert if an alarm is triggered during operating hours (08h00-18h00). Security Services will dispatch a patrol only in accordance with the Enhanced Call Verification procedure.
   (ii) If the alarm is triggered during silent hours, Security Services will dispatch a patrol immediately.
4.3.4 Subscribers who desire an intrusion alarm monitoring and response service outside of the hours set in Annex A may apply to Security Services for an exception. Applications will be evaluated on a case-by-case basis, and service charges may apply.

4.4 Alarm Monitoring of Personal Computer (PC) and Podium Tabs

4.4.1 Security Services will provide a 24/7 monitoring service for PC and Podium tabs alarms.

4.4.2 The type of response initiated during operating hours will be determined on a case-by-case basis, varying between executing the Enhanced Call Verification procedure and dispatching an immediate patrol. Alarms generated during silent hours will trigger an immediate security patrol dispatch.

4.5 Hold-up and Panic Alarms

4.5.1 Security Services will provide a 24/7 monitoring service for hold-up and panic alarms.

4.5.2 Upon reception of a hold-up alarm, Security Services will call 911.

4.5.3 Upon reception of a panic alarm, the Security Operations Centre will verify the camera on location to determine the nature of the emergency and provide the proper response.

4.5.4 If there is no camera on site:

(i) During operating hours, Security Services will call a contact number on site (not the workstation where the panic alarm was triggered) to determine the nature of the emergency in order to provide the proper response. If Security Services receives no answer, two patrollers will be dispatched.

(ii) Upon reception of a panic alarm during silent hours, two patrollers will be dispatched immediately.

4.6 Environmental Control Alarms

4.6.1 Security Services will provide a 24/7 monitoring service for environmental control alarms.

4.6.2 Security Services will respond to such alarms in accordance with the instructions provided. It is the responsibility of the subscriber to provide Security Services with up-to-date instructions and contact information.
4.7 False Alarms

4.7.1 One of the stated goals of this protocol is to reduce the incidence of false alarms because they result in unnecessary patrol dispatches and waste our security resources. An intrusion alarm is considered false when one or more of the following occurs:

(i) the alarm is caused by user error such as failing to enter the correct code to disarm the intrusion system or arming the system without ensuring that there is no one left in the alarmed area;

(ii) an unintentional activation of a burglar or panic alarm;

(iii) the alarm is caused due to an improper installation such as non-compliance with McGill design standards;

(iv) equipment failure;

(v) the alarm is caused by user negligence such as deliberately holding or propping open an alarmed door without making the proper arrangements with Security Services to mask said door or by failing to close a door that becomes unmasked at the end of the day; or

(vi) the alarm is caused by a maintenance operation where Security Services is not made aware of the work.

4.7.3 When applicable, subscribers are responsible for alerting Security Services after a false alarm has been triggered by calling the Security Operations Centre. The caller must provide a confidential password to confirm his/her identity.

4.7.4 Subscribers will be held accountable for excessive false alarms caused by user error/negligence or by failing to take the necessary steps to correct an equipment failure after being alerted by Security Services. For a complete list of subscriber responsibilities, please refer to the Service Level Commitment for Security Devices.

4.7.5 False alarm notifications are e-mailed to the subscriber representatives by Security Services. After three false alarm notifications within a 60 day period, Security Services may exercise its right of partial or complete withdrawal of its alarm monitoring service.

5.0 ROLES AND RESPONSIBILITIES

5.1 Security Services is responsible for management and operation of the central alarm monitoring system, and the development and implementation of standards relating to the
installation of security devices deployed on campus, as well as the response protocols to triggered alarms.

5.2 NCS is responsible for the maintenance of security device installations that are monitored by the University’s central alarm monitoring station.

5.3 The Service Level Commitment for Security Devices provides a complete list of support services provided to alarm subscribers and lists the responsibilities undertaken by the subscriber.

6.0 ANNEXES

Annex A: INTRUSION ALARM MONITORING BY ROOM TYPE

7.0 REVISION HISTORY

Amended:
30 October 2015 - Added clause whereby security device owners are obliged to inform Security Services if the room or space is remodelled, repurposed or allocated to new occupants; added a clause whereby the alarm monitoring service may be suspended if an installation does not comply with McGill design standards; modified the Intrusion Alarm Monitoring by Room Type grid.

Amended:
21 June 2012 - Added a definition of the term <Lock or Locked Down>.

Baseline Document:
18 November 2011
## Intrusion Alarm Monitoring by Room Type

<table>
<thead>
<tr>
<th>Room Type</th>
<th>Card Reader and Associated Door/Window Contacts</th>
<th>Intrusion System with Keypad</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alarm Monitoring on Weekdays</td>
<td>Alarm Monitoring on Weekends and Holidays</td>
</tr>
<tr>
<td>ACADEMIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditorium without equipment</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Auditorium with AV equipment</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Classroom without equipment</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Classroom with AV equipment</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Computer facility</td>
<td>Condition A 24 hrs. 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Library - Service Desk</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Library - Study Area</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Library Stacks</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Research Lab - Animal Care</td>
<td>24 hrs. (Condition B) 24 hrs. 24 hrs.</td>
<td>24 hrs. (Condition B) 24 hrs. 24 hrs.</td>
</tr>
<tr>
<td>Research Lab - Dangerous Storage</td>
<td>24 hrs. (Condition B) 24 hrs. 24 hrs.</td>
<td>24 hrs. (Condition B) 24 hrs. 24 hrs.</td>
</tr>
<tr>
<td>Research Lab - Special Equipment</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Teaching Lab</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>STAFF &amp; STUDENT OFFICE SPACES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Room without equipment</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Conference Room with AV equipment</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Mail Room</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Office</td>
<td>18h00 to 08h00 24 hrs. 24 hrs. 24 hrs.</td>
<td>24 hrs. (Condition B) 24 hrs. 24 hrs.</td>
</tr>
<tr>
<td>Student Association Office</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Waiting Room</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>FOOD &amp; LEISURE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eating Area</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Preparation Area</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Staff Lounge</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Student Lounge</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Kitchenette</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Gymnasmium</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Locker Room</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Museum &amp; Exhibition Space</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
<tr>
<td>Theatre Auditorium</td>
<td>Building’s silent hours 24 hrs. 24 hrs.</td>
<td>Building’s silent hours 24 hrs. (Condition B) 24 hrs.</td>
</tr>
</tbody>
</table>
## Intrusion Alarm Monitoring by Room Type (cont.)

<table>
<thead>
<tr>
<th>Room Type</th>
<th>Card Reader</th>
<th>Intrusion System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alarm Monitoring</td>
<td>Alarm Monitoring</td>
</tr>
<tr>
<td></td>
<td>on Weekdays</td>
<td>on Weekdays and Holidays</td>
</tr>
<tr>
<td></td>
<td>on Weekdays</td>
<td>on Weekdays and Holidays</td>
</tr>
<tr>
<td><strong>RESIDENCE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Study Room</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Common Room &amp; Leisure</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Laundry Room</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Residence Suite (student)</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Residence Suite (staff)</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Kitchen/Cafeteria</td>
<td>Condition A</td>
<td>Condition A</td>
</tr>
<tr>
<td><strong>MAINTENANCE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Janitor's Closet</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Porter's Office</td>
<td>Condition A</td>
<td>Condition A</td>
</tr>
<tr>
<td>Maintenance Workshop</td>
<td>18h00 to 06h00</td>
<td>24 hrs.</td>
</tr>
<tr>
<td>Mechanical / Electrical Room</td>
<td>16h00 to 06h00</td>
<td>24 hrs.</td>
</tr>
<tr>
<td>Telecom Closet</td>
<td>Condition B</td>
<td>24 hrs.</td>
</tr>
<tr>
<td>Major Server Rooms</td>
<td>Condition A</td>
<td>24 hrs.</td>
</tr>
<tr>
<td><strong>OTHER</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio Video Conference Room</td>
<td>Condition B</td>
<td>24 hrs.</td>
</tr>
<tr>
<td>Stairs / Corridor</td>
<td>Condition A</td>
<td>Condition A</td>
</tr>
<tr>
<td>Elevator</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Garage / Indoor Parking</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>Toilette / Washroom</td>
<td>Never</td>
<td>Never</td>
</tr>
</tbody>
</table>

Condition A: Alarm monitoring depends on the facility’s hours of occupancy as some are occupied at all hours.

Condition B: Alarm monitoring is always, but when an alarm is triggered during operating hours, Security Services either (1) initiates the Enhanced Call Verification procedure where a patroller is dispatched only after two attempts to contact the subscriber representatives have failed; or (2) alerts a subscriber representative via an automatic email.