# TABLE OF CONTENTS

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

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

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

4.0 PROTOCOL

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>General Access</td>
<td>3</td>
</tr>
<tr>
<td>4.2</td>
<td>Card Access to Buildings during Silent Hours</td>
<td>4</td>
</tr>
<tr>
<td>4.3</td>
<td>Key Control</td>
<td>5</td>
</tr>
<tr>
<td>4.4</td>
<td>Access to Restricted Areas</td>
<td>5</td>
</tr>
<tr>
<td>4.5</td>
<td>Special Events in a Building or on Campus Grounds</td>
<td>6</td>
</tr>
<tr>
<td>4.6</td>
<td>Removal of University Property</td>
<td>6</td>
</tr>
</tbody>
</table>

5.0 ANNEXES

Annex A: ACCESS CONTROL & SPECIAL EVENTS............................................. Page 7
1.0 PURPOSE

1.1 McGill University Security Services administers the University’s central security system, which includes the Lenel OnGuard access control system and the Medeco keyway system. The purpose of this protocol is to define a standard level of access control that will support the goals and mission of the University and provide for the safety and security of the McGill community and for the protection of University property.

1.2 It serves as the framework by which all keys and access credentials will be managed, issued, duplicated, stored, controlled, returned, replaced, and accounted for.

1.3 Everyone acting on behalf of McGill University must take responsibility for faculty, staff, and student safety, as well as the security of university physical space and the assets contained therein.

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.

2.2 It applies to any space leased by the University where the access control device is managed by Security Services.

3.0 DEFINITIONS

3.1 Access Levels – detail the rights granted to individuals to access areas via card readers. Access levels can be linked to schedules, and card readers can have more than one access level associated with them.

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.

3.3 Area Key Coordinator (AKC) - a designated person within a department or faculty responsible for managing its keys by requesting, issuing, recovering, and tracking via appropriate records.

3.4 Badge - a credential used to gain entry to an area having automated access control entry points. See also <Proximity Card>.
3.5 Building Director - a designated person responsible for applying policies related to access, safety and security, and building use. The Building Director is the default Area Access Manager, Area Key Coordinator and authorized Medeco key requestor for the building.

3.6 Card Access 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. The system also enables automatic locking and unlocking of specific doors or groups of doors at prearranged times. An access control system usually replaces a traditional key system.

3.7 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.

3.8 Controlled Area - is defined as a room, office, building or other form of facility to which access is monitored, limited or controlled. Admittance to a controlled area is limited to persons who have official business within the area. See also <Restricted Area>.

3.9 Guest – a non-McGill person who has been invited into a University building but has not been given a McGill proximity card.

3.10 Key - a mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area

3.11 Key Holder - any University employee, student, volunteer, alumnus, service provider or visitor authorized to be in the possession of a key that accesses a University space.

3.12 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.

3.13 Master Key - A key that fits or opens more than one door. There are several levels of master key, each with different capabilities and rules for issuance and use (e.g., master key, sub-master key, grand-master key).

3.14 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>.
3.15 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) the McGill Service Provider ID card for employees of contracted firms working at McGill; and (3) a blank proximity card for temporary employees and visitors.

3.16 Restricted Areas - A restricted area is a room, office, building, or other form of facility to which access is strictly controlled. Admittance to a restricted area is limited to personnel assigned to the area and personnel who have been specifically authorized access to the area. Access control to a restricted area is more severe than a controlled area. See also <Controlled Area>.

3.17 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 <card only> 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>.

3.18 Unlock – a card reader or electric lock setting that unlocks the door permitting unfettered access. During this setting, the light on the card reader is green.

3.19 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 - also known as a card holder or key holder.

4.0 PROTOCOL

4.1 General Access

4.1.1 No unauthorized person shall prevent access to or egress from University property to anyone who has a right to such access or egress for legitimate purposes.

4.1.2 No unauthorized person shall interrupt any authorized activity or event or prevent any legitimate movement of persons.

4.1.3 Faculty, staff, students and McGill Service Providers must carry their McGill proximity cards at all times. Security Services personnel have the right to request the presentation of identification cards from anyone on University premises and may deny access to or require that any person unable to produce an identity card leave certain University premises.
4.1.4 The McGill proximity card remains the property of McGill University. No person shall lend his/her card to another.

4.1.5 A McGill issued key remains the property of McGill University. No person shall lend his/her key to another.

4.1.6 The awarding of access to controlled and restricted areas is the responsibility of the Area Access Manager (AAM). The Security Services website contains a list of all card readers and their respective AAMs.

4.1.7 The provision of blank access cards should be issued only to those who are ineligible for a staff or student McGill identification card or McGill Service Provider ID card. The use of blank access cards is governed by the Blank Access Cards Terms and Conditions of Use.

4.1.8 The provision, duplication and distribution of internal keys are controlled by the Building Director, and all requirements for keys must be submitted to his/her office. In practice, this responsibility is often entrusted, in part or in whole, to appointed Area Key Coordinators (AKC) if a building houses different faculty or service departments.

4.1.9 The provision of access should be kept to the absolute minimum and should be if there is a real and continuing need. While some academic buildings are available to students 24/7, access to office buildings and other controlled areas should be restricted only to those users who require access outside normal operating hours. The award of 24/7 access should especially be judicious.

4.1.10 Lost access cards and keys must be reported to the responsible department and to Security Services.

4.2 Card Access to Buildings during Silent Hours

4.2.1 The awarding of access to buildings during silent hours is the responsibility of the Building Director. For most buildings, operating and silent hours are established by the Building Director in conjunction with Building Services.

4.2.2 During silent hours, everyone is required to produce, upon request by a security agent, a valid McGill University proximity card. Any person unable to produce a proximity card or prove their authorized access will be asked to leave the premises.

4.2.3 Permission to have guests varies from building to building and is established by the Building Director. Where guests are permitted, they must be escorted by an authorized user at all times.
4.2.4 It is the responsibility of the user to secure any exterior door they open after the closing hours of that building.

4.2.5 Contractors working in the building must be escorted by a security agent hired for the purpose. If the Building Director or Area Access Manager authorizes the contractor to perform the work unescorted, he/she will coordinate and grant the access to the building for the contractors. Security Services must be notified of the arrangement or contractors found unsupervised or without a valid access card will be evicted.

### 4.3 Key Control

4.3.1 Building Directors / Area Key Coordinators are responsible for tracking the distribution of internal keys. At all times, they must be able to account for all assigned and unassigned keys.

4.3.2 Unassigned keys and masters keys must be secured in a locked key press.

4.3.3 In the event of a lost key, re-keying is recommended. The user or department will be held responsible for the cost of the changes required. If a department declines to re-key, it shall be noted. The matter will be a factor in any theft investigation and application to apply for reimbursement of lost or stolen property.

4.3.4 Any request for extra keys or to change locks must be submitted to the Facilities Call Centre by the Building Director or Area Key Coordinator.

### 4.4 Access to Restricted Areas

4.4.1 A number of areas are strictly off limits to all students and staff with the exception of designated University Services and IT staff members. Some of these areas include, include but are not limited to:

i. mechanical and electrical rooms;
ii. telecom and server rooms;
iii. heating and ventilating plant rooms
iv. service tunnels;
v. elevator machine rooms; and
vi. building rooftops.

4.4.2 Users requiring access to these areas must submit their requests to Facilities Building Operations and/or Network and Communications Services as applicable.

4.4.3 Some self-funded units manage their own facility rooms. Access requests to those areas should be directed to the controlling organization.
4.5 Special Events in a Building or on Campus Grounds

4.5.1 The use of University premises to hold events requires approval, and the approval process may vary depending on the proposed event as the use of space and facilities at the University is regulated by a variety of bodies.

4.5.2 Security Services personnel may refuse access or require individuals or groups to leave an area if no authorization has been given or if the individual or group refuses to respect the regulations of the University or any federal, provincial or municipal law or regulation.

4.5.3 Security Services reserves the right to add additional security personnel where it is deemed necessary at the expense of the event holder. See Annex A for more details.

4.6 Removal of University Property

4.6.1 During silent hours, security agents have been directed to prevent the removal of equipment (tools, desktop computers, etc.) from University premises unless Security Services received advanced written notification from the Building Director or Area Access Manager, stipulating the individual's name and type of equipment authorized for removal, including make, model and serial number.

5.0 ANNEXES

Annex A: ACCESS CONTROL & SPECIAL EVENTS

6.0 REVISION HISTORY

Amended: 09 March 2018 – Modified to include information on McGill Service Provider proxy cards and restricted use of blank access cards.

Access Control and Special Events

In assessing the need for additional security requirements, the following will be considered:

- Type of event (lecture, demonstration, party or concert).
- The nature of the event and any risks involved.
- The number of people expected at the event.
- Past experience with the event.
- The location where the event will be held. Consideration must be given to the ease of securing or containing the event.
- Attendance of V.I.P.’s. If so, will external law enforcement agencies be providing security for the V.I.P. or will the University security personnel be required to protect/escort these persons?

Security Services reserves the right to impose additional security requirements as we deem necessary.

Should event organizers not respect the conditions as instructed by Security Services, the event may be cancelled or shut down.