# TABLE OF CONTENTS

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

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

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

4.0 APPLICATION

4.1 Acquisition ........................................................................................................ Page 2
4.2 Conditions of Use .............................................................................................. Page 2
4.3 Protocol for AAMs ............................................................................................. Page 3
4.4 Protocol for Cardholders .................................................................................... Page 4

5.0 REVISION HISTORY ........................................................................................... Page 4
1.0 PURPOSE

1.1 Blank access cards are proximity cards without photo issued to persons ineligible for a staff or student McGill identification card. The purpose of this document is to outline the terms and conditions of use under which they may be employed with the Lenel OnGuard System at McGill University.

2.0 SCOPE

2.1 The terms and conditions of use outlined in this document apply to all University entities and any non-university entity under contract with the University that employs blank access cards in conjunction with the Lenel OnGuard System.

3.0 DEFINITIONS

3.1 Blank Access Card – a colloquial term used for a blank proximity card used at McGill University. Blank access cards have no photo (blank). There are two models currently in use:

3.2.1 the card; and

3.2.2 the fob (a small plastic electronic device that attaches to a key chain). Fobs are restricted for certain applications only.

3.2 Proximity Card - a generic name for contactless integrated circuit devices used for security access. McGill University currently uses three types of proximity cards for access control:

3.1.1 the McGill staff and student icard with photo;

3.1.2 a blank proximity card for temporary employees and visitors; and

3.1.3 the McGill Service Provider identification card for employees of contracted firms working at the University.
4.0 APPLICATION

4.1 Acquisition

4.1.1 All blank access cards must be purchased through Security Services as they are part of the University's security system it manages. The cost will include material, programming labour, and peripherals. Rates are available from Security Services. A one-year replacement warranty due to demagnetization is included.

4.1.2 Requests will take up to five (5) working days to process. For demands above 100 units, requestors should order well in advance of their anticipated need.

4.1.3 The only authorized requestors permitted to purchase blank access cards are building directors and area access managers (AAMs). All others will have to order through one of the above.

4.1.4 Orders can be placed using the appropriate form found on the Security Services website.

4.1.5 Blank access cards are electronic keys. As part of the loss control program, Security Services reserves the right to query requestors regarding the number of cards ordered or accumulated over time.

4.1.6 Blank access cards will be programmed into the Lenel OnGuard System using a standard naming convention established by Security Services.

4.2 Conditions of Use

4.2.1 Blank access cards may be issued for:

i. visitors (academic, student, professional; hospitality);
ii. casual employees;
iii. short term contractors; or
iv. as temporary replacement card for students, staff and faculty.

4.2.2 Blank access cards may not be issued for:

i. long term service providers (use the specific MSP ID card instead); nor
ii. as a long-term substitute for a McGill ID card with photo.

4.2.3 Fobs are restricted to key rings held by Security Services on behalf of University Services; for Building Services' key rings, and for hospitality use.
4.3 Protocol for AAMs and Staff Responsible for Blank Access Cards

4.3.1 Maintain a current inventory of all cards, ideally controlled by no more than two people. A sample inventory template is available for your use on the Security Services website. The inventory list should be reviewed regularly to ensure the information is current.

4.3.2 There must be enough information on the inventory form to be able to identify and track down each cardholder:
   i. the badge number;
   ii. the cardholder’s first and last name;
   iii. contact number; and
   iv. the cardholder’s parent organization or association with the issuer.

4.3.3 Use a sign out & sign in procedure whenever a blank access card is issued. The control sheet should include the terms and conditions of use for the cardholder. A sample control sheet template is available for your use on the Security Services website.

4.3.4 Where applicable, a recommended safety deposit of $20.00 should be levied for each blank card issued. Cardholders must sign and understand that they must return the card.

4.3.5 Issuance should be systematic and need-based and be kept as infrequent as possible, with consideration given to hours of work, work space, alternatives, frequency, urgency, and sensitivity of the space to be accessed. Restrict the usage of programming cards on “access always” by limiting the access levels with activation/deactivation dates in the assign wizard of Lenel OnGuard AAM.

4.3.6 The inventory list and control sheets (or equivalent) are subject to audit by Security Services.

4.3.7 Once a blank access card has been issued to an individual, notify Security Services of the cardholder’s name, so we can assign it to the card. Unfortunately, the Lenel AAM application does not permit you to do this. Similarly, when the card is returned to your inventory or reassigned, notify Security Services of the change. The appropriate forms are available on the website. **NOTE:** This protocol does not apply where blank access cards are employed for hospitality guest use.

4.3.8 Blank access cards have a renewable five (5) year life span. Track your card’s expiry date and request it be renewed when appropriate.
4.4 Protocol for Cardholders:

4.4.1 Blank access cards are keys. Do not lend them to anyone.

4.4.2 Blank access cards must always be kept in a secure location.

4.4.3 Lost and stolen cards must be reported to Security Services immediately (Downtown: 514-398-3000; Macdonald: 514-398-7777) so they can be deactivated.

4.4.4 Be aware of people following you through a secured door or other entrance without using their own card. This can happen either with or without your knowledge and/or consent.

4.4.5 All blank access cards must be returned to the issuer after the end date in order to be reused and recycled.

4.4.6 Ensure you understand the terms and conditions of use listed above.

5.0 REVISION HISTORY

Amended:
30 August 2013 – Modified the service delivery time on blank access card requests to account for the auditing process of each request.

Amended:
23 June 2011 – Modified the requisition process.

Baseline Document:
28 February 2009