McMaster University

Administration Policy

Complete Policy Title: **Electronic Access Control Policy**	Policy Number:
Approved by: **President and Vice-Presidents**	Date of Most Recent Approval:
Date of Original Approval: **May 2020**	Supersedes/Amends Policy dated: **New**
Responsible Executive: **AVP and Chief Facilities Officer**	Enquiries: **Security Services**
DISCLAIMER: *If there is a discrepancy between this electronic Policy and the written copy held by the Policy owner, the written copy prevails.*	

Preamble

McMaster University manages building access through an approved authorization process which is intended to allow door entry and exit to authorized users only. Access to campus space is controlled in some instances with keys (see Key Control Policy), and some with electronic access, for which this policy will apply. The process manages and records electronic card access through a standardized Card Access Request Form and Control System.

McMaster University (the "University") recognizes the need to promote and maintain a safe and secure environment for students, staff, faculty and visitors and maintaining a card-based building access system is part of the security process. This Policy is intended to protect McMaster University property, prevent crime and deter unlawful or inappropriate activity including unauthorized entry. Specific emphasis is placed on access to sensitive areas and those of ongoing research.

Each department of the University is responsible for administering access to their space and equipment. The departments will be responsible to authorize card access to the departmental space and equipment, allowing and restricting individual access. Departments of the University should regularly review access listings, to ensure only current employees have the appropriate access available to them. Departing staff should be removed upon completion of their work with the department.

Security Services will be responsible for administering access to building perimeters, as outlined in the Core and Premium Service Policy (See Appendix A), that are currently equipped with card access points, and will work in cooperation with departments in support of their requirements for future card access to building perimeters which will be funded by Facilities Services if they don't already exist.

The installation or removal of equipment, and the use, alteration and access to information contained within the Card Access Control System, will be carried out in accordance with this Policy.

The use of the Card Access Control System results in the electronic collection of personal information in the form of usage of the card and records the access activity of the individual utilizing the system. The University's administration of the Card Access Control System will be in carried out in accordance with this Policy, the

Freedom of Information and Protection of Privacy Act ("*FIPPA*"), and applicable Federal legislation and related University policies.

This Policy is intended to maintain the integrity of the Card Access Control System at McMaster University. Accountability for all access cards issued is paramount to the personal and physical safety and security of McMaster University's staff, faculty, students, contractors, and visitors. Further, the Card Access Control System is a vital component in the protection of buildings, infrastructure, and assets for McMaster University.

The Policy is intended to:

- Regulate Card Access Control including approved authorization, access card issuance, monitoring and recording of activity on properties owned or occupied by the University,
- Enhance public safety, prevent and deter crime, restrict unauthorized access, reduce the perceived fear of crime, reduce the cost and impact of crime,
- Protect University owned and/or operated property and buildings including but not limited to building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, and cashier locations,
- Restrict access to and control of University records retained in departments of the University in support of protection of privacy.
- Improve the deployment of and response by Security Services Special Constables that are supported by electronic monitoring of the Card Access Control System,
- Ensure that the installation and Card Access Control System equipment meets the needs of the University, and
- Ensure there is an appropriate process and program to manage the maintenance, operation, support, upgrade, and replacement of access control points.

Scope

This Policy applies to all card access control equipment hardware, software and infrastructure operated by McMaster University.

For the purpose of this Policy, the University environment includes University land and buildings; both on the main campus or any off site or satellite locations that are occupied by the University; this includes rented or leased properties occupied by McMaster University with the exception of the McMaster University Medical Centre (MUMC). Security for MUMC is provided by Hamilton Health Sciences.

All existing uses of the Card Access Control System on campus shall be brought into compliance within 24 months of the approval of the Building Access Control Policy through collaboration between departments with Security Services. The related costs to bring systems into compliance will be evaluated by Security Services and Departments.

Security Services recognizes that some off-site facilities may be governed by other access control processes specific to their location, such as the Waterloo Regional Campus, Kitchener. Requests for exceptions to this policy for off site locations are to be directed to and registered with Security Services.

Responsibilities

Security Services is responsible for the Card Access Control System and to ensure the proprietary Card Access Control System complies with the terms and conditions of this Policy.

Security Services will:

- Electronically monitor all Card Access Control locations and maintain a suitable monitoring station in a controlled, high-security area with access restricted to Security Services personnel only,
- Ensure that all card access system data is recorded and stored on secure computer servers and kept in a controlled-access facility,
- Ensure that the implementation and operation of all Card Access Control Systems comply with this Policy,
- Ensure all personnel monitoring the Card Access Control System are appropriately trained and supervised,
- Ensure cards reported lost or stolen are deactivated immediately and the incident recorded on an incident report,
- Maintain the ability to allow access,
- Report incidents where inappropriate access may be suspected to involve a privacy breach,
- Provide Card Access Control System reports and records when requested by McMaster Security Services for legitimate security purposes and in compliance with FIPPA legislation and this Policy,
- Administer this policy in conjunction with the Facility Services Policy on Core and Premium Services (Appendix A),

Security Services Technology Administrator will:

- Ensure the installation of systems is completed under the guidance of Security Services and in accordance with this policy while maintaining the University technology standards,
- Ensure the safe and secure storage of all Card Access Control System information,
- When requested by a department, conduct a documented operational audit of the Card Access Control System program,
    I. This audit will include providing departments with a list of persons authorized to have access to their department premises as they request,
    II. Produce a list of those persons that have access approval or multiple cards for review and response by the department.

Security Services Technology Administrator will NOT:

Provide Card Access Control System activity reports or records to any requesting department without the approval of the Director of Security Services or the Senior Manager of Security Services.

Audit logs are not to be used for random supervision of employees or access to areas when there is not a formal investigation commenced or bona fide reason provided and approved by the Director of Security Services.

Installation Responsibilities

All Card Access Control installation and upgrade requests must be submitted via Mosaic Work Order Request. These requests will be reviewed by the Technology Administrator who will determine access control requirements and ensure compliance with technical standards of the University. The Technology Administrator may consult at any time with the Senior Manager of Security Services if required,

Installation of Card Access Control equipment will be paid for in compliance with the Facility Services Core and Premium Services Policy (Appendix A),

For reasons of effective monitoring, departments must use standard McMaster Security Service approved access control systems as currently supplied and supported via Axiom. Departments and Faculties of the University will not install unapproved systems without the express consent of the Director of Security Services. Non-standard systems that cannot be effectively maintained and are installed at the date of this policy will be reviewed with the department in question and plans put in place to migrate them to University standards over an acceptable period of time. The cost for this migration will be the responsibility of the Department and will be evaluated by Security Services and Departments together.

Installations and upgrades will result in the completion of a Memorandum of Understanding related to ongoing maintenance and support costs.

McMaster University Departments and Faculties

Administration

- Every department shall:
  - I. appoint a person(s) in the department who is responsible for coordinating Access Control Card issuance requests and is responsible for the administration of card access, including removing staff from the access list when they move to other departments, or outside of the University. for the department that will work in cooperation with Security Services, and
  - II. notify Security Services if the appointed person changes through retirement, resignation etc. and of their replacement

Requests to Security Services

- Request Access Control Card System installations or upgrades for their area by completing a Mosaic Work Order Request which will be reviewed by the Security Services Technology Administrator.

Responsibility for costs of installation and maintenance

- Purchase and Installation costs for perimeter security are the responsibility of Security Services. Cost for internal building installations and requirements are the responsibility of the department or faculty as outlined in Appendix A, Section 8.

- The cost of issuance of each card (both new and replacement cards) will be charged to the Department or Faculty

- Maintenance and Support costs for hardware associated with the Card Access Control System hardware for each departmental will be identified as an ongoing cost to the Department or Faculty as identified in the chart at Appendix A. Costs may be adjusted periodically through the budget process under advice to departments.

New Card Issuance and Control

- Each department of the University is responsible for administering access to their space and equipment. The department will be responsible to track and authorize card access that allows and restricts individuals to their own department space and equipment.
- If a department has report generation or administrative access, Audit logs are not to be used for random supervision of employees or access to areas when there is not a formal investigation commenced or bona fide reason provided and approved by the Director of Security Services.
- Access Cards will only be issued to faculty, staff or graduate students who are members of the university community approved for access to the building, or space, in question. Undergraduate students will generally not be issued Access Control Cards. They may be provided to undergraduate students only as authorized a Dean, Assistant Dean, Chair or Associate Vice President. External parties who require access to space must be approved by a Dean, Assistant Dean, Chair or Associate Vice President, or, in the case of contractors, the VP Administration, AVP Facility Services or Designate Director or by the Facility Services Project Managers.
- Departments and Faculties may enter into a Memorandum of Understanding (MOU) with Security Services that authorizes the Department or Faculty to issue access control cards to persons only for areas, or parts of a building, they are responsible for and who are members of their department or faculty, including students,
- Departments or Faculties who do not issue access control cards themselves will enter into a Memorandum of Understanding (MOU) with Security Services who will provide access control cards and programming.
- Replacement costs for lost or stolen Access Control Cards are the responsibility of the department or faculty.

Audit

- Security Services will provide a list of Access Card approvals for each department upon request,
- Each department will review and update the list of Access Control Card approvals annually for return to S/S to Axiomrep@mcmaster.ca,

Issuing Access Control Cards and Access Authorization

Authorization requesting a person be permitted access will be completed by submitting electronically via email to axiomrep@mcmaster.ca.

Access Control Card and Related Costs

There are two types of Access Control cards. One with photo identification and one plain card without photo. All Access Control Cards are strongly recommended to have a preprogrammed expiration date except for full time, permanent faculty, and employees.
The appropriate card for issue will be selected and paid for by the requesting department. McMaster Security Services Technology Administrator is available to assist departments to select the best card for their needs.

Departments and Faculties can make individual decisions to issue photo or non-photo cards which can vary by card holder. The decision on which card to issue will vary the cost which is the responsibility of the Department or Faculty.

Non-Photo Cards with Number Identifier - $10.00
Photo Card with Name, Student / Employee Number and Photo - $20.00
These costs are subject to annual review through the Budget Process and changes will be advised to departments.

Access Control Cards without photos will have an expiry date pre-programmed along with the name of the person that has been issued the card. This information will be registered within the system. Access Control Cards can be renewed after the card has been expired to be used by the same person or provided to someone new.

If the department issues a card without a photo, the Department is responsible for establishing an issuance, audit, tracking and retrieval process that they will administer in order to protect their own department.

Access Control Cards will only be issued to:

- Faculty and staff members,
- Sessional and Teaching Assistants,
- Post-graduate students,
- Undergraduate students as approved by the Dean or AVP, and
- Visitors, contractors, and external parties as approved by the Department Chair, VP – Administration, AVP Facility Services or Designate Director or by the Facility Services Project Managers.

Authorized Access Card requests must:

- Identify the individual for whom the card is requested,
- Provide the access door identification and hours of authorized access,
- Identify an expiry date by which the card will no longer be required, and
- Provide an account code to which applicable costs/deposits can be charged.

Receipt, Return and Loss of Access Control Card:

- Individuals cannot give, lend, provide or transfer their issued card to be used by another person,
- The Access Control Card remains the property of the University,
- When no longer requiring the card, it must be returned to the issuing office or to Security Services It is the responsibility of the department to track the return of cards, either through reports or off-boarding
    - Lost or stolen Access Control Cards must be reported immediately by the card holder calling Security Services at extension 24281 for deactivation purpose AND ensuring that an incident report is filed with Security Services after business hours,
- It is the responsibility of the individual to report a Lost / Stolen Access Card and any unauthorized use of the card remains the responsibility of the individual until reported to Security Services.

Access Control Card Issuance to External Contractors and Visitors

- The Security Services Technology Administrator has authority to approve access to any individual as justified and reasonable.
- Contractors and visitors required to be issued an Access Control Card to any campus building must be approved by the Department Chair, Dean, VP, AVP or designated Director or Project Manager in Facilities Services.
- The contractor or visitor shall be issued and shall return Access Control Cards in accordance with this Policy.
- Each contractor or visitor issued an Access Control Card must have an end date pre-programed and cards will not be issued without this end date,
- The contractor or visitor is responsible for reporting lost or stolen access cards to the department Chair or Project Manager, who will immediately notify Security Services at (905) 525-9140 Ext 24281.

The individual who authorized the external Access Control Cards will remain responsible for tracking the issuance and return of the cards, including reporting loss or theft immediately. The cost of replacement, if required, will be charged to the Department or Project as the case may be.

Visitor Cards Issued by Departments

Departments that are authorized to issue Access Control Cards may issue a card to a visitor. Each card issued will be recorded in the appropriate log maintained by the Department and must be pre-programmed with an expiry date.

The department will remain responsible for tracking the use and return of visitor access cards, including reporting loss or theft immediately to Security Services.

Human Resources

Human Resources shall notify Security Services via axiomrep@mcmaster.ca of the need to remove Access Card approval for individuals resulting from resignation, termination, retirement, separation or any other reason that means that access is no longer required or permitted. Departments will email axiomrep@mcmaster.ca with any requirements for card cancellations.

Financial Costs

- Departments that are authorized to issue Access Control Cards to any person they approve are responsible for all costs associated with card supply, issuance, replacement, and programing.
- Departments who require that Access Control Cards be issued through Security Services will be charged for supply, issuance, programming, and replacement fees for lost or stolen cards,
- All costs associated with installation, maintenance and support of access control locations requested within a department or faculty area are considered premium security service and will be charged to the Department or Faculty through schedule found at Appendix A,
- Employees that have lost an employee card will be issued with a replacement card one time at no charge.

- Any subsequent loss will be charged to the employee at the replacement cost, not to exceed $20.

Access Control After Hours and During Closures

Those persons approved for access after-hours and during periods of closure will maintain their access at all times with no disruption of service until their card expires or they terminate employment.

For off-campus locations, Departments and site managers will need to ensure that appropriate arrangements for access are in place for persons who are authorized to enter the University buildings during designated closures.

I. Such authorization must be approved by the appropriate Dean or Director of Finance and Administration within each Faculty (AVP in the Faculty of Health Sciences) and include submission of an access control plan to Security Services and Environmental Occupational Health and Safety Services, by the Chair, Academic Director or Manager,
II. The AVP Facilities Services or Director may also approve access during closures,
III. All persons will comply with the McMaster University Risk Management Manual #344 entitled 'Working Alone Program' and will comply with the McMaster University Closure Policy.

Departments Booking Space for an Internal or External Client shall:

- To the extent clients do not have access to the space via their access card, make arrangements for access within their department through persons that are responsible for the space,
- Establish an access control plan for the event or activity,
- Communicate the access control plan 5 business days in advance of the event to Security Services clearly indicating perimeter access needs.

Disclosure of Access Control Information

- Information obtained through Access Control Card usage and monitoring shall be used exclusively for approved investigations, security, and law enforcement purposes,
- No attempt shall be made to alter any recorded information regarding Access Control Card.

Access Control information shall not be provided to anyone other than McMaster Security Services personnel except in the following circumstances:

I. For use at a formal University approved investigation or proceeding such as a Student Code of Conduct Hearing, Privacy Breach, University disciplinary processes, Grievance Arbitration and Provincial Tribunals,
II. Law enforcement agencies for the purpose of a criminal investigation or to assist in the identification of individuals relating to a criminal incident,
III. To comply with a Freedom of Information request unless an exemption under FIPPA applies,
IV. Other circumstances as approved by the Director of Security Services.

Non-Compliance with this Policy

Any non-compliance with this Policy by departments, individuals or third-party suppliers shall be reported to the Director of Security Services,

The Director of Security will review all reports of non-compliance and advise the Assistant Vice-President and Assistant Vice-President/Chief Facilities Officer with a recommendation on the appropriate resolution or sanctions.

Related Procedures or Documents

Freedom of Information and Protection of Privacy Act ("*FIPPA*")*,,*

RMM 344 Working Alone Policy.

APPENDIX A CORE AND PREMIUM SERVICES

Core Security

Core Security services include 24-hour, 365 days a year security presence on the main campus, including campus security patrols, investigations, monitoring of alarm systems, access cards, communications, emergency response, emergency notification and incident command. Security Services also works with the University community in the development of and participation in preventative initiatives.
Core Security is included in the Facility Services operating budget, and specifically includes,

1. Security Patrols available 24 hours per day including,
    - officers on proactive patrol in vehicles, bikes and on foot
    - front line security response to Calls for Service
    - front line security response to Emergency '88'
    - call taking, dispatch and CCTV monitoring
    - Building Lock Out Procedures
    - Emergency Lockdown Response
    - Daily Security Reports to University management

2. Issuing the initial Access Card for new employees

3. Investigations including complaint intake, interviews, report/court preparation and complainant safety planning
4. Infrastructure needed in monitoring and responding to all alarm systems,
    - Communications Centre Technology and Operations
    - Backup Security Control Centre
    - Management of the University Access Control and Access Cards
    - Base CCTV

5. Communications, including,
    - Management and Operation of the University 2-way radio system
    - Text and voice notifications of emergencies
    - Safety App for security – McMaster University Safety, Security & Transit - MUSST
    - Red emergency phones
    - Emergency response activation to calls to '88'
    - Monitoring alarms
    - Monitoring fire alarm systems

6. Emergency Response and Incident Command,
    - Emergency responses to alarms and other calls for service
    - Special Constable responses and investigations
    - Emergency notification systems, sirens, television displays, cell phone notifications and the MUSST app for cell phones
    - Lockdown sirens infrastructure, testing and maintenance

- Lockdown Procedure – Training, Signage, Exercise
- Nuclear Reactor – Emergency response planning
- Participation in the Crisis Management Group

7. Development and delivery of incident prevention initiatives including working with the campus community in a proactive manner focused on Crime Prevention Through Environmental Design (CPTED). Specifically, twice yearly university rounds with stakeholders that provide feedback on the physical security of the campus.

8. Working with departments on Violence Risk Triage focused on personal safety and compliance with Occupation Health & Safety in the workplace. Violence Risk Triage is a part of Core Security. The costs of completing a full Risk Assessments are to be assessed on a case by case basis and it may not be included in the core service.

Core security includes the planning, installation, maintenance, service, licence agreements and associated costs of ***perimeter security,*** technology systems as a fundamental safety requirement as identified by Security Services in consultation with Facility Services. This includes but is not limited to, access card readers and cameras at the building perimeter.

Premium Security

Premium Security services are additional services such as dedicated patrols, contract security services and staffing at special events. Premium Security includes any additional security requirements that are not included in core services. Premium Security services are operated on a full cost recovery basis. Examples of Premium Services include,

1. Dedicated Patrols required beyond Core Services
2. Provision and management of contract security guards
3. Services at buildings or locations that require special attention assignments
4. Additional staffing at special events
5. Cash transportations and/or escorts
6. Radio communications
7. Nuclear Reactor – Patrol, Alarm Monitoring, Emergency Response
8. Security technologies requested beyond base perimeter security, including additional CCTV, access control, panic buttons and installations in ancillary departments or locations.
9. Violence Risk Assessment cases requiring a full investigation will be dealt with on a case by case basis at the direction of the VP- Administration.

Premium Security Services	Cost
1. Dedicated Patrols required beyond Core Services.	Special Constable Hourly wage Average $29.35/hr
2. Provision and management of contract security guards.	$21/hr regular $50/hr stat/OT
3. Services at buildings or locations that require special attention assignments.	$45/hr
4. Additional staffing at special events	$45/hr
5. Cash transportations and/or escorts	$20/pick up/transport
6. Radio communications.	$42 per radio License cost % of Maintenance Agreement ($14,000) based on % use of system
7. Nuclear Reactor-Patrol, Alarm Monitoring, Emergency Response.	$30,000 yearly
8. Security technologies requested beyond base perimeter security, including additional CCTV, access control, panic buttons and installations in ancillary departments or locations.	CCTV-Install Charge $775/camera Yearly carrying cost $200/camera
	Access Point- Install Charge $200/unit Yearly carrying cost $20/unit
	Input- Panic Button Install Charge $120/unit Yearly carrying cost $10/unit
9. Violence Risk Assessment cases requiring a full investigation will be dealt with on a case by case basis at the direction of the VP - Administration	TBD

Security Services provides cash transportations and radio communications management on a cost recovery basis. These cost recoveries are administered through Memorandum of Understandings (MOU) with various University departments. The cost recoveries do not yet cover the full cost of providing cash transportations, but the agreements are moving in that direction.
Previously installed security equipment is evaluated as required and recommendations are made when new installations may be required to maintain best practices. Core Security does not include equipment replacement, new installations, or interior controls as requested by Faculty or the facility occupant. Monitoring of outdated and unsupported technology is not covered under core security. The cost of maintaining the current equipment is the responsibility of the faculty or facility occupant and any changes, alterations, upgrades or replacement must be made in compliance with the University standards as set by Security Services.