Draft Policy for Consultation

Building Access Control Policy

Feedback can be sent to Policy@Mun.ca

Purpose*:*

To establish authority, responsibilities, and procedures for the control of physical access to university buildings. This is to ensure that all university buildings are secure and for the protection of the university community and physical assets as needed.

Scope:

All Memorial University owned/controlled infrastructure and physical access control systems. This policy applies to all university employees, students, visitors, and all external organizations using, or contemplating the use of university facilities.

Definitions*:*

Access Control Program – the documented organization of doors and door groups assigned to units that that have associated key and electronic access. Including documented organization of key and electronic access assignments of university community members as requested through a departmental authority. This may be documented through electronic access control or key management systems or by manual records. Access control programs also require a risk register of all unit spaces and identified controls to enter high-risk spaces.

OCRO – Office of the Chief Risk Officer

Unit - Academic or administrative unit as defined in the University Calendar.

Unit Head - Deans, Department Heads, Division Heads, Heads of Schools, Directors, Executive Directors, University Librarian, University Registrar, and other senior administrators at a comparable level; Associate Vice-Presidents, Vice-Presidents, the President, as applicable.

University – Memorial University of Newfoundland

University Buildings – Space occupied and managed by Memorial University of Newfoundland, this may include owned space, leased space and space inhabited by the university under shared service agreements.

Policy:

General

The University is responsible for ensuring compliance with this policy and relevant procedures.

The OCRO is responsible for establishing the policy and procedures regarding physical building access for the university. The OCRO is guided by the Memorial University Access Control Procedure in executing its responsibilities.

The appropriate unit head will ensure each campus has an Access Control Program in keeping with the requirements contained in the Physical Access Control Procedure.

The position/unit responsible for facilities maintenance for each campus will also have the responsibility for maintaining all physical access control systems, including but not limited to: doors, frames, locks, keys, door and frame hardware, electrical and fiber optic cabling, and access control hardware and devices (e.g. proximity reader, electronic strike, door contacts/magnets, electronic latches, power transfer hinge, motion sensor, etc.).

Responsibility and accountability for controlling interior building spaces rests with the unit assigned those spaces, through any associated policies and procedures. The Unit shall undertake building access control measures as outlined in the procedure for building access and control and shall review all physical access every semester.

The access control program, as detailed in the procedures, will consist of documentation of building access control measures in keeping with the procedure and will be kept on file by the responsible units and reported to the OCRO.

Assurance

Records will be audited by the unit and the OCRO to maintain compliance with this policy.

Non-compliance with policy could result in the delay or removal of physical access granting authority.

Approval Date: *to be entered / updated once approved by the Board of Regents*
Effective Date: *insert date the policy comes into effect*
Review Date: *normally four years after the Board approval date; earlier if specified.*
Authority: The President
Sponsor: Vice-president (administration, finance and advancement)
Contact*:* The Office of the Chief Risk Officer

Related Documents
Space Policy

ACCESS CONTROL PROCEEDURE

Definitions:

Electronic access device Coordinator - the employee in the unit assigned the responsibility for coordinating electronic access device requirements and permissions within the unit. This is a functional description, not a position title.

Access Control System - refers to an electronic/electro-mechanical locking system that consists of hardware and software. Access privileges are controlled via software and door release/lock mechanisms are activated by the system based on electronic access device and associated access privileges

Access group - is a door grouping assigned to departments in the key and electronic access systems. Once a user is added to an access group, they will have access to all the doors in that access group.

Facilities maintenance unit - refers to the unit(s) at each campus responsible for management of facilities and capital work.

Change Key - a key which operates a single door or multiple doors in a building.

Departmental Authority - the responsibility held by an employee designated by the unit head to be responsible for authorizing access to buildings or interior spaces controlled by unit. The Departmental Authority holds oversight responsibility and accountability for the Key Coordinator and the Electronic access device Coordinator functions. This is a functional description, not a position title.

Electronic Access Devices - includes programmed cards, key fobs, and any other electronic devices that are programmed to disengage an electronic locking mechanism, thereby permitting access to a building or interior area that is otherwise locked.

Electronic Locking Mechanism - refers to a programmable locking device that requires power to operate (wired or battery), is activated by an electronic access device with a magnetic stripe or proximity chip and may have a key override.

Grand Master Key - a key which operates all door locks within the university campus each individual door lock having its own individual change key.

High Risk (Restricted): This level of security is the most sensitive. Additional safeguards, such as background checks, may be required before being provided access to Restricted

Intrusion Alarm System: uses motion sensors, door/window contacts, and other devices to detect an unauthorized entry into an alarmed area. The area is armed and disarmed with a code on a keypad device assigned to the room or building. It sends a signal to assigned security services when one occurs.

Key - a device inserted into a lock that allows the lock to be disengaged mechanically, thereby permitting access.

Key Coordinator – employee in a unit assigned the responsibility for key control, requisitioning, distribution, retrieval, and recordkeeping within the unit. This is a functional description, not a position title.

Key Holder – someone with a key or electronic access device.

Locking System – is any mechanical or electrical system that secures a door. The door can be locked or unlocked with a key or electronic access device.

Low Risk (Non-Restricted): Areas that do not have risks identified with access to the space as outlined on the access risk matrix. These areas still require authorization from the departmental authority to gain electronic access or to request keys.

Master Key - a key which operates all door locks within a building with each individual door lock in that building having its own individual change key.

Risk Matrix - defines the criteria for the risk's likelihood and severity, from insignificant to severe. It is also color-coded to show the priority of each of the risks charted on the matrix.

Risk Register – is used to document risks identified using the risk matrix. The access register details all room categories for the unit, description of the risk, inherent risk factors, the risk rating, the controls required and the residual risk rating. This is used to assess the risk of access to different spaces and place controls on the space to reduce the risk.

Submaster Key - a key which operates all door locks within a department within a building with each individual door lock in that building having its own individual change key.

ROLES AND RESPONSIBILITIES

The University

- The university shall ensure that the unit responsible for facilities and maintenance for each campus will be responsible for all physical installations of locking and access control measures in university buildings that restrict access to locked space. This includes, but is not limited to doors, frames, locks, keys, door, and frame hardware, electrical and fiber optic cabling, and access control hardware and devices (e.g., proximity reader, electronic strike, door contacts/magnets, electronic latches, power transfer hinge, motion sensor, etc.).
- The university shall ensure that the unit responsible for facilities maintenance is solely responsible for installations, repairs, or modifications to locks and associated hardware. Only those authorized by the university may install, repair, or replace any portion of an access control system.
- The unit responsible for facilities maintenance shall be responsible for central key production, issue, control of master keys, and distribution of regular/change keys and mater key rings to the units. They shall keep up-to-date records of:
    - Master Key (MK) and/or Submaster (SM) key holders across the University;
    - Mater key rings;
    - Keys manufactured for and given to the units to control.
- The university shall ensure that a common template for managing key control processes is implemented by every unit.
- The university is responsible for delegating assignable building space to units.

- The university shall maintain a current record of each departmental authority and the person responsible for electronic access control (Electronic Access Device Coordinator) and key control (Key Coordinator) in each unit.
- The university in partnership with the OCRO shall monitor the issuing of master keys and shall, from time to time, undertake an audit of all master key types.

Office of the Chief Risk Officer

- Establish and maintain university-wide guidelines and oversight of access control and related security system measures;
- Provide advice and recommendations to departments regarding the development and maintenance of access control systems and measures for their respective areas;
- Provide adequate communication and resources to all departmental authorities for the purpose of collecting information for Electronic Access Device distribution;
- Provide unit reports to designated authorities for departmental auditing of access control program, where applicable.
- The OCRO are responsible for conducting audits to ensure compliance with the policy and procedure.

Unit Responsibility

- Responsibility and accountability for identifying and controlling interior building spaces and recommending access to those spaces' rests with the unit.
- The Unit shall undertake this control in compliance with standards and procedures established by the University.
- Each Unit shall name a Departmental Authority responsible for access management and key control within their Unit. This person will have authority to request changes to locks and decide who gets access and ensure that the Electronic Access Device Coordinator and Key Coordinator functions are assigned.
- Ensuring that controls are in place for high-risk spaces as outlined in the University access control risk register.
- The unit shall ensure that the exit process for employees leaving the university is followed and that all keys for employees' no longer employees shall be returned and electronic access is revoked.
- A unit seeking an electronic or other access control system to replace a mechanical lock system shall request their campus facilities maintenance unit.
- Report lost or stolen keys and electronic access device within their unit using the online for reporting.
- In conjunction with the departmental authority, the space owner is responsible for auditing the access control program for their areas and departments each semester.
- Units that sponsor contractors, visitors and guests shall make all arrangements for access with the department(s) that are responsible for the space;

Housing Services

- Housing Services for each campus is responsible for managing, issuing, and maintaining all keys and electronic access device requests to residence buildings and student housing on each campus of the university.

Key/Electronic Device Holder

- People who have been issued with an electronic access device/key are authorized to use the electronic access device/key to gain access only to the areas and facilities necessary for the performance of their work/studies.
- Electronic access devices/keys are only used by the person to whom they were issued.
- People who have been issued with a university electronic access device/key accept responsibility for the:
    - appropriate and legitimate use; and
    - safe keeping.
- Electronic access devices/keys that are no longer required (e.g., when a person changes location within a unit or is no longer employed at the University) must be returned by the holder to their unit or line manager.
- Master Keys must be kept in person and not in offices unless they are held in a suitable key safe or approved electronic access device/key issuing system.
- Lost, stolen, damaged or found electronic access devices/keys must be reported immediately to the department / unit / University.

Procedure:

Access Structure

- Each campus shall maintain business hours to identify when they are open to the university community. Buildings will be locked and unlocked during these times.
- Perimeter doors to major buildings are preferably fitted with electronic access, with a manual master key over-ride system to primary perimeter doors.
- Access control guidelines must address the needs of faculty, staff, and students, including those with disabilities.
- Various areas or spaces on campus are deemed “High Risk” areas and have restricted access for general staff, students and maintenance staff because of the health and safety risks that these areas pose or because they house valuable equipment.

    Typical High-Risk areas include:
    - Student and on campus housing;
    - labs with biological, radiological, and chemical hazards
    - roof access and panels through external walls.
    - ITS data centers and data rooms
    - central utilities (mechanical, electrical and boiler rooms)
    - substations
    - rooms that house valuable/lucrative assets; and confined space zones.

- The framework for controlling and authorizing the issuance of keys and electronic access device is presented in the chart below:

Access Level (Key, Card, or Fob)	Use	Holder	Authority

Grand Master Key	Campus Wide - Based on Campus.	Security Services, Facilities/Building Management or Designated Authority for the Building.	Grenfell - Director of Facilities St. John's – Director of Security Labrador – Director Harlow – Director Signal Hill - Operations Manager
Master Key	Individual building	Security Services, staff,	Grenfell - Director of Facilities St. John's – Director of Security Labrador – Director Harlow – Director Signal Hill - Operations Manager
Submaster Key	Individual units in a building	Dean, Department Head, Administrative Assistant	Departmental Authority or Operating Unit
Change Key	Individual doors or set of doors keyed alike	Employees, visitors, contractors	Departmental Authority or Operating Unit
Perimeter Access	Entrance doors only	Employees, Facilities/Building Management, Security Services	Departmental Authority or Operating Unit, Campus

- Building entrance keys (for buildings without an electronic access system) and electronic access devices with after-hours authorization will be issued only to people with a demonstrated need for after-hours access to a building. This could include critical research, or access to services that require 24/7 oversight.
- The University's keying is established under a registered key system managed by the facilities and maintenance unit for the campus.
- Independent keying outside of the master key structure is not permitted.
- Lessees of University spaces are not to change University key or access system infrastructure unless authorized by the University.

Intrusion Alarm System

- Access control systems are not intrusion alarm systems. Units requiring specialized alarm response/monitoring for secure facilities should install an intrusion alarm system with the access control system if required.
- This service should be requested through the facilities maintenance unit assigned to your campus to ensure it is assessed using a physical security assessment and integrated with university infrastructure.

Request for Access / Key

- Employees and students requiring access to buildings shall be granted access only based on need due to their conditions of employment, program of study, or extra-curricular club or association. Any request for access must be from a designated departmental authority.

- Students living in residence are given standard building access to their associated residence building and interior access to the bed space they have been assigned.
- Electronic access control for students will expire at the end of each semester, unless otherwise informed by the designated authority.
- Any employees or student's access to a restricted space must meet all control measures and training requirements before access is approved.
- Employees on an employment term contract should only have access to the building for the term of employment and should expire once the term has ended and keys returned to their unit.

Request for Access - External Contractors, Visitors and Affiliated Organizations

- If an individual is not an employee or student of Memorial and requires building access the department responsible for the individual must request a means of access for that individual.
- Expiry dates are required on all access requested for visitors, contractors, and affiliates.
- Building Access and Interior access for residences building will be managed by Student Housing and Conference Services.

Revoking access

1) The university is authorized, on the direction received from the unit or for due cause to revoke/deactivate, at any given time, building access, or interior access to university managed facilities for any key or electronic access device holder.
2) At the university's discretion, building and interior access may be revoked/deactivated due to changes in department, faculty, individual business needs or misuse of an electronic access device.

Key and electronic access should be removed upon:

- Termination, resignation, or retirement;
- Completion of a fixed term of employment or contract,
- Completion of studies and research,
- Upon notification of a death, or;
- Upon contravention of this procedure.

Misuse of a Key or Electronic Access Device

Once issued, electronic access devices/keys are not transferrable. The individual to whom the electronic access devices/keys were issued is responsible for their security.

Misuse of an electronic access device or key can include but will not be limited to:

- Unauthorized propping open of locked doors;
- Purposely causing doors or locks o become inoperable;
- Transferring or loaning electronic access devices to unauthorized individuals;
- Attempting to duplicate electronic access devices, or keys;
- Unlocking doors for unauthorized individuals, except police, fire, or other public safety personnel during an emergency.

Lost or stolen keys and electronic access device

When an electronic access device is lost or stolen, it is the responsibility of all individuals that have knowledge of the incident, whether it is the device holder or report the access device missing.

- A lost or stolen key or electronic access device must be reported to the unit, or the local security unit for the campus and documented. In the absence of building security, the loss must be reported to the Unit.
- The university shall normally reissue a lost, stolen, damaged, or nonfunctioning key after the identity of the holder has been validated and a request has been submitted.
- The OCRO shall decide if key replacement or lock/cylinder change is required. The university and the OCRO shall together determine appropriate action should any type of master or sub master key be lost or stolen. If replacement is required, the expense is the unit's responsibility.
- The university will immediately disable all building access programmed on electronic access devices that have been reported lost or stolen.

Repairs and Changes to Physical Access Control Systems, Keys, and door hardware

- Routine maintenance of locks and lock cores is the responsibility of the university. These services are provided without charge.
- Specific or specialized security needs are met by providing alarm devices, electronic access locks, and other advanced locking devices. These categories of services will be charged to the user department.
- In exceptional cases such as space relocation, renovation or construction, capital/project accounts will be charged for locks installed, removed, or rekeyed as part of capital or departmentally- funded alterations projects.
- Upgrades required due to lost or stolen keys or a department's failure to maintain adequate key control will be charged to the department.
- Requests to replace keys shall be directed to the Departmental Authority of the unit.
- Any level of master key that is broken or damaged must be reported to CEP and shall be replaced by Campus. The university is under existing approval processes for the level of key, upon written request by the Departmental Authority. All damaged or broken keys must be returned to the university before the new master key is issued.

Device Return – Keys and Electronic access devices

- The unit shall ensure that the exit process for employees leaving the university is followed and that all keys for employees' no longer employees shall be returned and electronic access revoked.
- All students, staff and visitors to the university are permitted to keep their campus card as they are often used for other purposes in addition to building access. If the employee or student status changes a new card is required. All other electronic access devices shall be returned.
- All electronic access devices should be deactivated, have an expiry date, or have the access level removed once the access is no longer needed. It is the unit's responsibility

to ensure that all access in their department is managed properly each semester when they are no longer required.

- All keys must be returned to the university and will not be reissued within the department unless a key transfer request has been submitted to the facilities maintenance unit.
- Unidentified keys should be returned to the unit for identification and/or destruction by the facilities maintenance unit.

Assurance

Departmental/Unit Audits

- Reports will be sent to departmental authorities at the end of every semester of their electronic access device holders and annually of their key listings. It is the department's responsibility to ensure that all electronic access is up to date at the end of each semester and their key lists are updated annually and records are maintained.
- Keys that are lost or not returned to the university must be reported to the university.

Audit of Program

- The OCRO may conduct access audits for compliance purposes, as necessary. All authorized approvers must comply with periodic or random audits. Audit reports shall be generated and shared with relevant stakeholders to track and address any non-compliance issues promptly.
- The Physical Access Control Procedure shall be reviewed at least annually and updated as needed to reflect changes in standards and operations, and the evolving security landscape of the university.

Appendix A – Risk Matrix

		RISK MATRIX - ACCESS	
		SEVERITY	
		Low	High
FACTORS	Health and Safety	First aid, medical aid	LTI, Permanent disability and fatality
	Financial	<250K in property damage or stolen assets	>250K in property damage or stolen assets
	Reputational	Stakeholder or multiple stakeholder complaints	Stakeholder or multiple stakeholder complaints; extremely sensitive information
	Recovery	1-3 days to recover	4-10 days (about 1 and a half weeks) to recover

Appendix B – Risk Register (Example)

Risk ID	Category	Description of Hazard/Risk	INHERENT RISK FACTORS				Access Control Level	Controls	Residual Risk Rating
			Health and Safety	Financial	Reputational	Recovery			
EHS_Access-RA-R12	Classroom/Teaching Facilities	First aid	Low	Low	Low	Low	Low		Low
EHS_Access-RA-R17	Research/Laboratory Facilities - Laboratories Teaching/Laboratory Facilities - Laboratories	Chem/rad/bio exposures, stolen equipment, or IP	High	High	High	High	High	Training, Restricted access	Low
EHS_Access-RA-R18	ITS - Data/Server rooms	Data Leak, critical system downtime, brand damage	Low	High	High	High	High	Restricted Access, Intrusion Detection, Cameras, Training	Low
EHS_Access-RA-R19	FAS - select spaces								Low
EHS_Access-RA-R20	Registrar's office - select spaces								Low
EHS_Access-RA-R21	HR – select spaces								Low
EHS_Access-RA-R22	Presidents/VP offices								Low
EHS_Access-RA-R23	Storage (Bitters, Breezeway, food bank, dining hall, GeoCenter)								Low
EHS_Events-RA-R29	Central services (server)								Low