

UTM Access & Key Control Program

The main purpose of this program is to enhance the personal safety of our community members and to protect property of the University of Toronto Mississauga. Two aspects are critical in achieving this goal: maintenance of accurate records, and efficient control for mechanical keys and electronic access credentials. The long-term view for the University of Toronto Mississauga Campus Police is to have all buildings secured in the most effective manner possible.

Access Control at UTM consists of two categories: mechanical key and electronic access. This program covers both.

I. Definitions

ACCESS CARD – A University of Toronto issued credit card sized item used to gain entry into a controlled location.

ACCESS CONTROL - Control of entry/exit to an area by any means (mechanical or electrical).

ACCESS CONTROL DIRECTOR – Manager of Campus Police, responsible for overall operation of campus security including all levels of access control

CARD ACCESS CONTROL - Access control system using electronic or electromechanical devices to replace or supplement mechanical key access (normally a credit card style device).

CARD ACCESS CONTROL FILE - Records maintained by the Campus Police Services – Card Access databases.

ACCESS CONTROL SYSTEM - A high capacity computerized card access control system replacing or supplementing mechanical key system to control access to an area. The system is managed by the UTM Campus Police Services and uses access cards (normally a credit card style or occasionally fobs) to unlock doors. This system can also be used to provide automatic locking and unlocking of specific doors or groups of doors at prearranged times.

ACCESS CREDENTIALS – either mechanical key or electronic card/fob used to access secure area.

DEPARTMENT ACCESS AUTHORIZER (DAA) - A full-time staff person in a given Department appointed by the Departmental Head (Dean/Department chair/Director) to be responsible for the adherence and implementation of this program. The department DAA will update UTM police, as to any changes to the DAA, by January of each year, or as the changes arise.

DEPARTMENT ACCESS AUTHORIZER DESIGNATE (DAA designate) - A full-time staff person in a given Department appointed by the Departmental Head (Dean/Department chair/Director) to be the authorized designate so DAA's duties can be performed during his/her absence.

MASTER KEY – a mechanical key that unlocks more than one door within a geographical or operational boundary (departmental master keys, building master keys, mechanical master key, etc.). Note, UTM areas are keyed to a well-defined master/sub-master system to efficiently control spaces within UTM buildings. In this document, all master and sub-master keys are referred to as master keys.

MECHANICAL KEY - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area.

MECHANICAL KEY CONTROL FILE – Records maintained by Facilities Management & Planning – Key recipient databases.

MECHANICAL KEY SYSTEM - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area.

SECURE AREA – any area that is to be locked with either mechanical key or electronic card.

SECURE KEYBOX – A Keybox approved by UTM Campus Police for secure storage of Departmental sub – master keys.

II. Process

To update Tcard access, modify door opening schedules or install a new electronic card access system, a request **MUST** be submitted by the Departmental Access Authorizer (DAA). The request is to be submitted through the UTM Service Now Portal https://uoft.service-now.com/utm_access . Campus Police will review all requests and respond within 3 business days. **Please note:** Submission by the DAA must include specific information such as the person's UTORID, building, and room number/s for which access modifications are required.

To update, modify or install mechanical key/locks, a request has to be submitted by the Departmental Access Authorizer (DAA). The request is to be submitted through the UTM FM&P Work Order system (https://uoft.service-now.com/utm_fmp), and FM&P will review all requests and respond within 5 business days. Please note: submission by the DAA must include specific information such as the building name, floor, and room number/s for which keys are required.

To request a security keybox installation within a department, please submit a request through the UTM Service Now Portal https://uoft.service-now.com/utm_access

III. Responsibilities

CHIEF ADMINISTRATIVE OFFICER: with the assistance and advice from the Manager, Campus Police, the CAO approves modifications of existing and installations of new large scale campus wide systems (both mechanical and electronic).

MANAGER, CAMPUS POLICE: is designated as the overall Access Control Manager. Issuance of all master & Departmental sub master keys must be approved by the Access Control Manager.

ASSISTANT MANAGER, PHYSICAL SECURITY, CAMPUS POLICE: is responsible for managing the UTM card access systems to ensure safety and security to end users occupying buildings or facilities:

1. Coordinating new system installations and upgrades.
2. Makes changes to access card right's upon request from the Departmental Access Authorizers
3. Programs new and existing door schedules for doors equipped with card access readers upon advance notification from DAA's

DAA: has the ultimate responsibility for maintaining records of the access credentials for the department and efficient communication with Campus Police.

1. Maintain accurate records of all access control and key distribution activities.
2. Submit requests for new and modified access credentials for all faculty, staff, students, and research personnel within his/her department.
3. Recover University access credentials from personnel who leave UTM.
4. Report any failure to recover keys and access control cards to Campus Police.
5. Notify Campus Police of all persons who no longer require access to secure areas.
6. Lost or stolen keys must be reported to Campus Police & FMP.
7. Submit requests 3 business days in advance for door schedules changes to support internal and external room bookings (ensures there are no duplicate requests submitted). **Please note:** ORBS bookings will reserve the room **ONLY**, and will not result in any Tcard reader state changes with the **exception** of the **IB building on weekends**.
8. Administer department keybox access assignments and will update UTM Campus Police regularly.

DAA DESIGNATE: performs DAA duties when the DAA is not available.

DEPARTMENT HEAD: The department head shall appoint a member of his/her department to be responsible for the duties of the DAA and shall advise the Assistant Manager, Physical Security in writing of the DAA and his/her designate. The notification should include the members' work location, email, and telephone number.

ALL UTM COMMUNITY USING ACCESS CREDENTIALS:

1. Maintain and use all access credentials in responsible manner.
2. Report loss or theft of their access credentials to their DAA and Campus Police within 24 hours of discovery of theft or loss, and
3. Return all access credentials upon leaving the University (graduation, termination of employment, etc.).
4. No one shall have, use, lend, borrow or duplicate access credentials unless specifically authorized to do so.

IV. DOOR HARDWARE, CARD ACCESS CONTROL SYSTEM UPGRADES AND MAINTENANCE

REQUESTS: All requests for installation or modifications to access card reader(s) shall be submitted by the DAA to the Assistant Manager, Physical Security Campus Police. All requests for modifications to existing locks shall be submitted through work order system to FM&P.

REVIEW: All requests for additional security devices must be reviewed and approved by the Manager, Campus Police. Each request will start with a review of user needs and a security survey of the affected facility by Campus Police, FM&P, and I&ITS. The review will conclude with recommendations on the type and placement of equipment & devices.

APPROVAL: All large projects that impact overall campus wide access control have to be approved by the CAO. Additions and modifications to the system have to be approved by the Access Control Manager. Changes to individual door locking mechanisms have to be approved by the Assistant Manager, Physical Security, Campus Police.

INSTALLATION: All physical installation of hardware (both mechanical and electronic) once approved is to be carried out by FM&P. System and element programming once approved is to be carried out by Campus Police.

REQUEST FOR SERVICE: All requests for service of electronic access hardware, whether emergency or routine, shall be made through the Assistant Manager, Physical Security. All requests for service of mechanical locks, whether emergency or routine, shall be made through work order system, FM&P.

ROUTINE TESTING: All equipment will be tested by Campus Police or Service Contractor on an annual basis. Proper use of the equipment will be reviewed with the user Department at the time of each test.

KEY AUDIT: FM&P or Campus Police reserves the right to request a key audit from any UTM Department to ensure that access credentials records are accurately maintained.

V. FUNDING RESPONSIBILITY

Please be aware that the following charges apply to mechanical keys:

- Exterior keys have \$20 deposit which will be refunded once the key is returned (cash only).
- Vivarium access cards have \$10 deposit which will be refunded once the key is returned (cash only).
- Medeco keys have \$20 charge for a replacement (cash only).
- Medeco master keys or sub-masters if lost may incur significant costs associated with rekeying. These costs will be charged to the department.

Regular maintenance and upgrades on UTM general doors is the responsibility of UTM. However, special locks or locks installed at specific user requests have charges associated with electronic keys:

- Costs related to maintenance and repairs of existing hardware.
- Costs related to software testing.
- Costs related to new installations.
- Charges to UTM departments will be based on actual costs (no markup).

VI. MASTER KEYS

Requests for all master keys must be submitted by the DAA and approved by the Access Control Manager.

The following general guidelines are to apply:

- Each department will be issued 2 sub-master keys to access areas within their own space allocation. These keys are issued to the DAA and/or the chair of the department, and **MUST** be stored in a UTM approved secure key box (not taken off campus).
- Building master keys will not be issued.
- Real Estate style lock boxes for Department key storage will NOT BE permitted, and will be removed if found by UTM Campus Police
- Keys to unlock Tcard enabled doors will not be issued.
- Mechanical master keys will not be issued. For repair work, renovations, etc. keys can be signed out at the Campus Police, with the approval of the Manager, Mechanical Operations.
- IITS master keys will not be issued. For repair work, renovations, etc. Access must be approved by the IITS engineering group, who will make access arrangements.
- Support space master keys are not to be issued. For repair work, renovations, etc. keys can be signed out at the Davis Building 3rd floor corridor keybox after pre authorization is granted through an FMP PM responsible for each external contractor.

Medeco master keys if lost, will require re-keying of all lock cylinders for associated doors in the building, therefore may incur significant costs that will be charged to the department (based on prevailing market rates).

For questions regarding mechanical keys, please contact the UTM Helpdesk at 905-828-5344 or Myron Kulykowsky at 905-301-2218 (Acting Assistant Director Building Operations and Services) or email M.Kulykowsky@utoronto.ca

For questions regarding electronic access control, secure key boxes and overall campus safety & security, contact Steven Rivera, Assistant Manager, Physical Security, W.G. Davis Building Rm 3116 or, email at Steven.Rivera@utoronto.ca.

Appendix 1.

- Construction keys will be issued only to awarded contractors for each project. A \$75 deposit applies. The deposit will be refunded once the keys are returned. Keys will be available for sign out, at the FMP, keys office