THE UNIVERSITY OF WINNIPEG

Procedure Title:

Key and Electronic Access Control Procedures

University Classification & Procedure Number:
TBD

Approval Body:
University Administration

Responsible Designate:
Vice President, Finance and Administration

Established:
2022

Revised:
Not applicable

Editorial Revisions:
Not applicable

Scheduled Review:
2027

1.0 Procedure Purpose

The purpose of these procedures is to establish and clearly define the principles for authorizing, monitoring and controlling access to University facilities in accordance with the Key and Electronic Access Control policy.

2.0 Definitions

The following definitions apply to terms as they are used in this Procedure document:

2.01 "Access" refers to the permission given to enter a building or space.

2.02 "Access Card" refers to a card with a programmed chip in it that provides access to a physical space via a reader.

2.03 "Authorized User" refers to any individual who has been issued access to University Facilities.

2.04 "Building Key" refers to a key that operates all locks in a building.

2.05 "Credential" refers to an access card, key fob, mobile app and/or pin code.

2.06 "Designated Authority" refers to the Department Chair/Director/Head and/or a respective designate in each department or unit who has been designated to authorize access to individuals in their specific area(s).

2.07 "Electronic Access Control" refers to the technology used to provide and deny access to a physical space.

2.08 "Physical Security Platform" refers to the technology used to manage the access control and intrusion alarms in the University Facilities (Salto and Genetec).

2.09 “Floor Key” refers to a key that operates all locks on one floor of a building.

2.10 “Primary Key” refers to a key that operates locks in multiple buildings.

2.11 “Key Fob” refers to a small secure hardware device with a built-in authentication programmed to provide access to a physical space via a reader.

2.12 “Pin Code” refers to a personal identification number that will arm and disarm a security alarm panel for a building or an area of a building.

2.13 “Reader” refers to an electronic device that reads one or more types of credentials and converts the information into a coded data stream that it passes to the panel for interpretation.

2.14 “Room Key” refers to a physical key that can operate a single lock.

2.15 “Sub-Department Key” refers to a key that operates one group of locks within a building.

2.16 “University Facilities” refers to all buildings and spaces owned and/or leased by the University of Winnipeg.

3.0 Scope

3.01 The procedures outlined herein apply to all members of the University community, including faculty, staff, students, contracted service employees, and visitors, and includes all University owned or leased properties. Maintaining effective access measures and physical security platforms that manage them are critical to ensuring the security of our physical infrastructure, personal safety of individuals and research being conducted.

4.0 Procedure Elements

4.01 Issuing of Keys and/or Electronic Access Control Credentials:

a) All requests for keys and electronic access control credentials shall be submitted to the Facilities Management office on a standard key and electronic access control requisition form. These forms can take up to five business days to process.

b) All key and access control requisition forms must be signed by a Designated Authority. Department Chairs/Directors/Heads are the Designated Authority for their areas. They may also delegate the authority to a respective designate by sending a Designated Authority form to the Facilities Management office. Designated Authorities should authorize access at an appropriate level taking into consideration factors such as the employee or student’s needs, personal safety, and activities.

c) The Designated Authority is responsible for ensuring all necessary safety training is completed prior to allowing access to rooms with specialized equipment.

d) Once authorized by all Authorizing Officers, the Facilities Management office will communicate to the Designated Authority or the Authorized User when the keys and electronic access control credentials are ready to be picked up.

e) All requested keys and electronic access control credentials must be picked up within thirty days of the request being processed unless prior arrangements have been made. Any

unclaimed keys, access cards or key fobs will return into inventory. If access is still required after that period of time, a new key and electronic access control requisition form will need to be submitted.

f) Non-regular employees and students must pay a one-time $20 deposit for any physical key or access card they receive from the Facilities Management office. This deposit will be refunded when all keys and/or access card issued to them have been returned to the Facilities Management office.

g) Setting up expiry dates for electronic access control credentials will be required for all students and term employees including Contract Academic Staff. If an extension is required, a new key and electronic access control form will need to be submitted to the Facilities Management office.

h) Some departments will be given permission to program electronic access control credentials for their own students / faculty / staff / clients. Departments will have access to update the Authorized User's profile with a sub-set of doors on the physical security platforms. The doors they are authorize to give access to will be determined by the Facilities Management department.

4.02 Lost, Stolen or Otherwise Missing Keys / Electronic Access Control Credentials:

a) Authorized Users must report lost, stolen or otherwise missing key(s) and/or electronic access control credentials to the Facilities Management office or Security Services immediately.

b) The Facilities Management department or Security Services will deactivate the credential in the physical security platforms. Security Services must advise the Facilities Management Department of any lost stolen or otherwise missing keys and/or access credentials.

c) Prior to re-issue, the individual must complete a new key and electronic access control requisition form. The individual will be required to pay a replacement fee for each key and/or electronic access control credential lost or stolen. Non-regular employees and students will need to pay a new deposit that will be refundable upon return. Fees are as follow:

i. Keys - $20.00/key

ii. Access Card - $20.00

iii. Key Fob - $20.00

d) The Facilities Management department will review the key(s) lost, stolen or otherwise missing to determine which locks must be re-keyed. If the Facilities Management Department deems it necessary to re-key a space, floor or building for security reasons it will be re-keyed at the expense of the department or unit that lost the key.

4.03 Key and/or Electronic Access Control Retrieval:

a) All keys and electronic access control credentials issued remain the property of The University of Winnipeg and shall be returned under the conditions described below:

Employees:

i. upon transfer to another department;

ii. upon relocation to a different office or building;

iii. upon termination of employment;

iv. upon the request of the department Chair/Director/Head; OR

v. upon commencing a leave of absence for a period of 30 days or longer. An employee on such a leave may retain their key if that employee is authorized to have access to the building and/or office during the leave

Students:

i. at the end of the academic session or period after which the keys will not be used for at least 30 days; OR

ii. upon the request of the department Chair/Director/Head

b) It is the Designated Authority's responsibility to retrieve the Authorized User's key(s) and or access control credentials under the conditions described above. The Authorized User can also return their key(s) and or electronic access control credentials to the Facilities Management Office.

c) If a Designated Authority retrieves keys from an employee or student under the conditions described above and wishes to transfer them to a new employee, they will need to send a new key and electronic access control requisition form to the Facilities Management office requesting the key transfer. Otherwise all keys must be returned to the Facilities Management office.

d) The Facilities Management department will deactivate an individuals' electronic access control credential from the physical security platforms based on the Human Resources Employee Update Report that is sent on a bi-monthly basis.

4.04 Roles and Responsibilities:

a) Facilities Management Department

The Facilities Management department is responsible for:

i. Maintaining the key management database to track all keys issued to Authorized Users. The database must be capable of tracking when keys were issued and returned.

ii. Ensuring the physical security platforms in the University Facilities are maintained.

iii. Reviewing, approving and issuing keys and electronic access control credentials requested taking into consideration factors such as the employee or student's needs, personal safety, activities, and security.

iv. Ensuring the integrity of the key schedule and the schedule of all electronic door locks.

v. Assessing the need to re-key a space/floor/building.

vi. Working with the Planning Office to determine keying needs during construction projects.

vii. Ensuring the proposed hardware meets the University and accessibility standards:

- All classrooms / Seminar Rooms / Meeting Rooms Laboratories, etc. have electronic access control locking mechanisms in place for safe havens in the event of an emergency.
- Main departmental entrances, departmental administration offices, mail rooms and common areas have electronic access control.
- Mechanical rooms and wiring closets have electronic access control.
- All other doors have Abloy keys.
- Work in consultation with Accessibility Services and the Planning Office to ensure accessibility standards are met.

viii. Reviewing and approving which departments can have access to issuing electronic access control credentials to Authorized Users. Departments will be granted this permission based on the following conditions:

- The doors / spaces are under their sole program responsibility.
- Mechanical / electrical / custodial / data closets are excluded.

b) Security Services

Security uses the physical security platforms to assist the Facilities Management department to re-issue access control credentials after hours. They will ensure the following requirements are adhered to:

i. Ensure individuals using the physical security platforms have been trained and understand the importance of granting access.

ii. Individuals using the electronic physical security platforms must be issued their own User ID. Sharing User ID's is not allowed.

iii. Reviewing Authorized User profiles and make recommendations based on safety and security concerns. These recommendations can't be implemented until they have been reviewed and approved by the Facilities Management department.

iv. Assist with adjusting the electronic door locks schedule to accommodate the following circumstances:

- University Closures (i.e. statutory holidays).
- Special Events (temporarily restricting access).
- Emergency events.

v. Performing audits on access as part of an investigation.

c) Departments Issuing Access Control

In order to be granted authority to issue electronic access control credentials, departments must ensure the following requirements are adhered to:

i. Ensure individuals using the physical security platforms have been trained and understand the importance of granting access.

ii. Individuals using the physical security platforms must be issued their own User ID. Sharing User ID's is not allowed.

iii. Have a defined approval process for what access within their control is granted to the Authorized User, including an expiry date for the access.

iv. Departments are responsible to ensure that the Authorized User's access is deactivated when access is no longer required.

v. If the Authorized User has an existing profile:

- The department will update the profile with the access they wish to grant.
- The department is responsible for removing only the access they granted from the profile when it is no longer required.

vi. If the Authorized User doesn't have an existing profile:

- The department will create a profile to grant access.

- The department should use the University issued ID card if available. If not, they may issue a new access card.
- The department is responsible for removing access from the profile when it is no longer required.

vii. Departments are responsible for covering the cost of the electronic access control credentials they issue.

5.0 Related Policies, Procedures and Institutional Documents

- Key and Electronic Access Control Policy
- Access to University Buildings and Property Policy
- Working Alone / In Isolation Policy