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

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 securitreturill2 (he psd) an 9.2 (i)-8.9 (l)3.1 (l)-8.9Tj -0.00. (r)-6.4 . (r)-6.4 . (r)lursecterlc

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