



Key and Access Card Control

University Policy No.: BP3125
Classification: Building and Properties
Approving Authority: VPFO
Effective Date: March 2017
Supersedes: January 2010
Last Editorial Change:
Mandated Review: March 2024

PURPOSE

- 1.00 The purpose of this policy is to ensure authorized access and security of all University facilities and to maintain the integrity of the key, access card distribution and collection, and door access privileges while effectively addressing the needs of the community users for appropriate access to university space.

Accountability for all keys and cards issued is paramount to the personal safety and physical security of the university's staff, faculty and students as well as being a vital component in the protection of assets for the University and its various departments and faculties.

DEFINITIONS

- 2.00 Card/Door Access System is an electronic locking system that provides building and door access control.
- 3.00 Master Key is a unique key or access card that operates one group of locks or locking devices within a building.
- 4.00 Grand Master Key (Building Master) is a key or access card that will open all doors within a designated space, such as a building.
- 5.00 Great Grand Master Key is a key or access card that operates multiple locks or locking devices for multiple buildings.
- 6.00 University Buildings are buildings identified on the university campus map that comprise the Gordon Head Campus and includes Ian Stewart Complex.

JURISDICTION/SCOPE

- 7.00 This policy applies to all locks and Card/Door Access Systems to doors of all University Buildings.

POLICY

- 8.00 The use of unauthorized locks or Card/Door Access Systems on university owned property or buildings is strictly prohibited.
- 9.00 Individuals are prohibited from unauthorized possession, duplication, disabling, programming or circumventing of locks and/or card access systems to university facilities. This includes, but is not limited to filing keys, or modifying cylinders or locks. The propping of doors to bypass security and taping latches is also prohibited.
- 10.00 All keys and access cards, for the use and access to University Buildings and property remain the property of the university and shall not be duplicated or shared.
- 10.01 Assigned key(s) must be returned to the university upon termination of employment or when the need for access is no longer required.
- 10.02 Door access privileges will be revoked by the university upon termination of employment or when the need for such access is no longer required.

New and/or Additional Locks/Card/Door Access Systems

- 11.00 All requests for the installation of new or additional locks and/or Card/Door Access Systems to University Buildings and property must be made in writing to the Executive Director, Facilities Management or delegate. The Executive Director, Facilities Management will consult with the Director of Campus Security to review safety and security related issues and to ensure compliance with University of Victoria policies and procedures.
- 12.00 The custody and control of all door hardware to the doors of all University Buildings is administered by the Executive Director, Facilities Management or delegate. The Facilities Management Department is responsible for the selection, installation, management and maintenance of all the university's centrally administered Master Keying and Card/Door Access hardware and controls.
- 13.00 Keys and Card/Door Access Systems associated with new building and renovated space will be charged to the project account. Costs associated with other key issues, lock changes or Card/Door Access System changes requested by departments will be the responsibility of the department.

Keys and Access Cards

- 14.1 For the general use and administration of keys and access cards, the following conditions apply:
 - 14.2 The Executive Director, Facilities Management, or delegate, is responsible for the approval and distribution of keys.

- 14.3 Department heads are responsible for the distribution, handling, control and custody of keys, and access card privileges issued to them by the Executive Director, Facilities Management or delegate.
- 14.4 Should a request for keys and/or card/door access systems be disputed, a request may be made to the Vice-President Finance and Operations. Each request will be assessed for security and safety related issues and any other issue that cannot otherwise be resolved.
- 14.5 The Great Grand Master Key, the Grand Master Key and Master Key are restricted keys and will only be issued on a demonstrated need basis.
- 14.6 Only one key or access card will be issued or assigned per person for a specific lock or Card/Door Access System.
- 14.7 All stolen or lost keys must be reported immediately to the Director, Campus Security via written correspondence. Stolen or lost access cards must be deactivated immediately, either online or by contacting the ONECard Office.
- 14.8 The Executive Director, Facilities Management and/or the Director of Campus Security may, from time to time, arrange for a review of a department's procedures for security, distribution, assignment and retrieval of keys and access card privileges.
- 14.9 All obsolete, broken or other unnecessary keys shall be returned to the Facilities Management Department immediately.

Restricted Keys

- 15.00 "Master" keys will only be issued on a demonstrated need basis and will require the approval of the Director, Campus Security or delegate, or the Executive Director, Facilities Management or delegate for keys required by Facilities Management staff.
- 16.00 All Great Grand Master keys shall only be authorized by the Director of Campus Security or delegate and be hand-delivered by Campus Security.
- 17.00 Campus Security will be responsible for maintaining the recordkeeping system for the issuance of Great Grand Master keys. All Great Grand Master keys shall be signed for by the recipient.
- 18.00 The issuance of Master Keys shall normally be restricted to two per Department and will only be authorized by the Director of Campus Security or delegate.

Card/Door Access Systems

19.00 The following conditions apply to Card/Door Access Systems only:

- 19.1 The installation of a Card/Door Access System may be considered for authorization in areas where:
 - 1) there are multiple users; and
 - 2) users are expected to change frequently (i.e. every semester); or
 - 3) there is a need to limit access for reasons of safety, where the safeguarding of assets is required or other considerations.
- 19.2 Card/Door Access Systems are restricted to the interior space assigned to the department. Exceptions will be granted at the discretion of the Director, Campus Security in consultation with the Executive Director, Facilities Management.
- 19.3 Assignment of access card privileges within a designated space (i.e. department) is the responsibility of the department to which the Card/Door Access System has been assigned.
- 19.4 The Executive Director, Facilities Management, or delegate, is responsible for the maintenance of hardware associated with Card/Door Access Systems. University Systems is responsible for managing and maintaining the central door access server and application software. All costs (excluding card readers and access control panel) associated with the maintenance of Card/Door Access Systems are the responsibility of Facilities Management. Card reader and access control panel costs are the responsibility of the requesting department.

AUTHORITIES AND OFFICERS

- i) Approving Authority: Vice-President Finance and Operations
- ii) Designated Executive Officer: Vice-President Finance and Operations
- iii) Procedural Authority: Executive Director, Facilities Management
- iv) Procedural Officer: Executive Director, Facilities Management

RELATED POLICIES AND DOCUMENTS

Building Usage policy BP3105