George Brown College Public Safety & Security

Key Request Guide

Standard Key Requests

For standard key requests, the Department Access Key Controller (DAKC) must complete a key request form indicating:

- The number of keys
- The area(s) the key(s) and doors will access
- To whom the key(s) will be assigned
- The reason(s) for the key request
- This form is then to be emailed to accesscontrol@georgebrown.ca

Regular and Emergency Requests

REGULAR: Requests are usually completed within five days.

EMERGENCY: The second level of request is an "emergency" that requires action quickly.
In these cases, the DAKC should call the Public Safety office and explain the situation to determine if it qualifies for emergency response. If it does, the DAKC must immediately email or fax a copy of the completed key request form to the Public Safety office and a service call will be made to the locksmith during which time security precautions will be initiated.

Replacing Lost Keys

When a key is lost, the person who lost the key must make a Lost Key Report with Security, and contact their DAKC. The report takes only a few minutes and can be made over the telephone with Security at Ext: 8000. The DAKC, requesting the replacement key(s)/re-key(s), must prepare a new key request.

Why a Key Request Might Be Delayed

There are several instances in which a key request may be delayed:

- Persons requesting a large number of keys/re-keys.
- Unclear and/or incomplete information on service request.
- Persons requesting a replacement for a lost key when no Lost Key Report has been made to the Public Safety office.

In all cases, Public Safety office staff will contact the requester when their key request is delayed. See the following section on Key Controller's for more information on designated authorized key requesters.

Key Controller

George Brown College Public Safety Division requires that each department have one designated Key/Access Controller (referred to as the DAKC) who orders and tracks keys and has ultimate responsibility for the department's access.
This ensures that there is no duplication in requests and facilitates solid inventory control and record keeping at the department level.
An alternate key controller, fully oriented to the department's key control system by the Key Controller, is allowed to assist .
Only three individuals have signature authorization for the department's service requests for keys/re-keys: the department head (dean/department chair/director), the Key Controller, and the alternate key controller. Their printed names and signatures must be listed on a Public Safety Key Control Authorization Form on file with Public Safety Division prior to any approval of service requests.
The Public Safety and Security Division must be notified whenever there are changes in the DAKC, the alternate, or the department head.

Record Keeping

DAKC's must keep a record of when and to whom the keys are issued to for areas in the department. This helps the Key Controller manage access control more effectively.
A department can create its own form or log if needed. All records for keys should be kept as long as the key is still in circulation and for one year after the key is no longer in circulation.
Please contact the Access Control Specialist at Ext 6518 if you would like assistance in developing a record keeping system.

Requesting Keys from Former Employees

Anyone who no longer works for the department is required to surrender his/her department keys to the Department Access Key Controller.

Key and Re-Key Approval Checklist

Complete key request form:

- Requester's name, work phone, date of request, department, campus location
- Service Description
  1. Number of keys
  2. Key(s) assigned to
  3. The area(s)/rooms(s) that the keys/re-keyed doors access
  4. Reason for keys
- Authorized Key Controller/Alternate Key Controller/Department Head's name

Approval and Information Contact Numbers

For key and re-key approvals, or for answers to questions about automated access control, contact

Access Control Specialist Steven Rivera at: srivera6@georgebrown.ca

Campus Access Control Program

Policy

The one overriding purpose for this policy is the protection of the lives and property of the George Brown College community. Maintaining accurate, effective access control - with both metal keys and electronic devices - is critical to protecting the College. The majority of thefts occur without forced entry, so it is imperative that proper access control is maintained. The long-term view for the College is to have all buildings controlled with electronic card keys.

This policy is in place to ensure that people requesting access cards and keys actually are authorized to do so; to ensure a process of accountability for return of access cards and keys.

The method to update card access and key requests is relatively simple: The person who needs their access updated or keys makes a request to the person in their department who controls access. When the Department Access Key Controller needs access updated or keys, they request it at accesscontrol@georgebrown.ca

The policy is applicable to current and future GBC sites under the operational jurisdiction of George Brown College. It applies to access control systems installed in new construction or as part of any major or minor capital improvement project.

I. Description

Access Control at George Brown College is divided into two (2) categories: mechanical key, and card access control.
.
A. MECHANICAL KEY SYSTEM - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area.
B. CARD ACCESS CONTROL SYSTEMS - A high capacity computerized card access control system operated by the Public Safety & Security Department. An electronic or electromechanical device replaces or supplements mechanical key access. Card keys (normally a credit card style) are used to unlock doors. Access to specific doors by individuals, is determined by the Department Access Key Controller.
The system provides entry access to various doors within a building. Provides automatic locking and unlocking of specific doors or groups of doors at prearranged times during the day.

II. Definitions

A. ACCESS CONTROL - Control of entry/exit to an area by any means (mechanical or electrical).
B. DEPARTMENT ACCESS KEY CONTROLLER - A full-time staff person in a given department appointed by the Department Head to be responsible for the adherence and implementation of this policy.
C. CARD ACCESS CONTROL - Access control system using electronic or electromechanical devices to replace or supplement mechanical key access (normally a credit card style device).
D. KEY - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area.
E. KEY CONTROL FILE - Records maintained by the Public Safety & Security Department - Key & Access Databases.
F. ACCESS CARD – A George Brown College issued credit card sized item used to gain entry into a controlled location.

III. Responsibilities

A. **The Manager, Public Safety & Security** is designated as the overall Access Control Director and is responsible for the following items:

1. In consultation with the VP Corporate Services, approves all access control systems and modifications to existing systems.
2. Reports the results of key/card control record audits of campus departments to the VP of Corporate Service, at regular intervals.

B. **Access Control Specialist:** is responsible for managing the College's card access, and keying systems to ensure security and convenience to department's occupying buildings or facilities and for coordinating new systems.

Their duties include:

1. Maintains card/key control, access systems, and records.
2. Updates and modifies new and/or existing access cards and places key service fabrication orders upon request from departmental DAKC's.
3. Consults with Manager, Public Safety & Security (or designee) concerning records of access cards & keys lost or stolen. Decisions to rekey or to duplicate keys are based on consultation between the Manager, Public Safety & Security, and the respective Department Head. All rekeying will be administered through the College's approved Locksmith. The cost of rekeying and key-cutting is borne by the affected Department.

C. **The Department Head** shall appoint a member of his/her department to be responsible for the duties of the Access Key Controller and shall advise the Manager, Public Safety & Security, in writing, of the departmental member assigned the responsibilities of access key controller, and their alternate. The notification should include the members' work address, telephone number and signature (for future verifications).

D. **The Department Access Key Controller** is responsible for developing adherence to and implementing the following:

1. Maintain accurate records of all access control activities,
2. Order and issue all department access control keys, and access card updates,
3. Recover College access control cards and keys from personnel who leave the College.
4. Report any failure to recover access control cards and keys to the Access Control Specialist.

E. **All GBC** personnel are required to do the following:

1. Sign their names in the "Issuance of Keys", section of the key request form.
2. Maintain, secure and be responsible for any access control key(s) issued,
3. Report loss or theft of access control card or keys to the DAKC, and to the Public Safety Division within 24 hours of discovery of theft or loss, and
4. Return all access cards and keys issued to the DAKC upon leaving the College.

Any person/s whom knowingly makes, duplicates, possesses, or uses access control (cards/keys) to GBC premises, without authorization-from the Public Safety & Security Division, is in violation of this policy:

No individual locks/keys may be used for space control, nor may locks be changed without approval of the Department Head and the Manager, Public Safety & Security. Unauthorized locks will be removed by order of the manager, Public Safety & Security at the expense of the person or affiliated group in charge of that room. Unauthorized push button combination locks will be confiscated and replaced with a standard key operated lock at the expense of the person or affiliated group in charge of that room.

IV. CARD ACCESS CONTROL SYSTEM UPGRADES

1. Requests: All requests for installation of access card reader/s shall be submitted by the department head to the Manager, Public Safety & Security.
2. Review: Each request for a new card access control reader or modifications to existing systems will result in a security survey of the facility (or facility plans) by the Public Safety & Security Division. The survey will include recommendations as to type and placement of equipment and detection devices.
All requests for additional security devices such as alarm service must be approved by the Manager, Public Safety & Security.
Once approved, the Department requesting the new security devices can proceed with a web requisition to Manager, Public Safety & Security.
3. Orientation of the User
a. The Public Safety & Security Department shall meet with the Department Access Key Controller and/or their designees to develop the security clearances and schedule of door operation.
4. Issuing of Cards
a. The Library will issue all new staff, and student ID cards.
b. The DAKC shall complete, and sign a card access form for each access card update request sent to Public Safety & Security.
c. The Public Safety & Security Division will update in their computer all access request updates or modifications within 5 working days. Emergency requests for immediate updates will be accommodated when phone contact is made with an authorized DAKC. The written application must be sent within 24 hours of the phone request.
d. Lost or Stolen card access keys/cards, shall be reported to security, and the DAKC within 24 hours of discovery of the theft or loss. The Public Safety & Security Division shall remove all lost or stolen card access keys from an active state. Written documentation shall be forwarded to the Public Safety & Security Division by the issuing department for all lost or stolen cards/keys.

5. MAINTENANCE, REPAIR AND REPLACEMENT

a. **Requests for Service to Access Control Hardware:** All requests for service, whether emergency or routine, shall be made through the Access Control Specialist at Accesscontrol@georgebrown.ca

6. Testing: All equipment will be tested by the College Access Control Specialist or Service Contractor on a semiannual basis. Proper use of the equipment will be reviewed with the user department at the time of each test.

7. Modification and Removal of Service

a. Approval for Modifications: Approval must be obtained from the Public Safety & Security Department prior to any modifications to an existing system. Approval is necessary to ensure continued compatibility with Security equipment.

Approval and Information Contact Numbers

For key and card access updates, or for answers to questions about automated access control, contact:

Access Control Specialist Steven Rivera at: srivera6@georgebrown.ca