***Updated:  September 20, 2009***

# STONEHILL COLLEGE

## Academic/Administrative
## Access Control System
## Operational Protocols

## Introduction

This document contains operational protocols for the access control system at Stonehill College. Although some of this document is technical in nature, the primary goal is to develop standard access control systems for the campus which allows for ease of operation while still remaining flexible enough to meet the various access needs and still provide the highest degree of security possible. For issues relating to key control, please see the Facilities Management Key Control Policies which can be found on the Facilities Management Website.

In order to achieve this goal, it is necessary to assign responsibility for the electronic access control card(s) to the individual users. In reference to these protocols, electronic access control card(s) are defined herein as "keycards". Designated perimeter and interior doors are outfitted with centrally controlled electronic access control system components. Keys for access control doors will only be issued to designated police officers and locksmiths, as a means to manual override these control systems.

## Responsibility

Given the number of buildings and the many individuals needing access to same, it is imperative that rules and guidelines governing the issuance of keycards and the approval of individuals to receive keycards be clearly stated and consistently enforced. Control over cards is established through the joint efforts of the

(1) Director of Campus Police; and
(2) the Division Heads;

Director of Campus Police: Upon written request by a Division Head, an individual may be designated as a Card Authorizer for a specifically defined area within a building or buildings. Once so designated, a Card Authorizer will be added to the master list of Card Authorizers maintained by Campus Police. When Card Authorizers cease to be employed by the College, or for other reasons cease to be the Card Authorizer for a given area, the Division Head as named above shall authorize another individual to act as Card Authorizer for that particular area, and submit this information in writing to the Director of Campus Police. The Department of Campus Police being advised of this change in Card Authorizers' will update the list accordingly. A similar procedure will be followed whenever the space utilized by an organizational unit within the college changes and the occupancy of space changes such that one or more Card Authorizers' jurisdictions change.

Card Authorizers: By virtue of this designation, a Card Authorizer may approve requests for access to rooms in their defined area of authority by submitting written request to the Director of Campus Police. Card Authorizers are NOT authorized to approve requests for areas outside their defined area of authority.
Authorizers are responsible for maintaining records, as needed, to meet internal departmental needs, to include at a minimum a listing of all access granted and currently outstanding. Also, they are responsible for insuring compliance with these guidelines

among card holders and others, especially in prohibiting the exchanging or loaning of cards.

Card Holder responsibilities: Anyone to whom a card has been issued is a card holder. Card holders are the only ones allowed to use the cards and are responsible for maintaining custody of the cards issued to them at all times. Failure to maintain custody of cards compromises the security of persons and property. Violations of these policies may be grounds for serious disciplinary action. Card holders are expressly forbidden from exchanging or loaning their cards to anyone else, or to accept custody of some other card holder's card. Card holders must take reasonable measures to protect their cards from theft, loss or unauthorized use. Any inappropriate use of cards by card holders may result in the immediate surrender of the card. If a card is lost, the card holder must report this to the Department of Campus Police immediately so that appropriate measures can be taken to maintain the security of both the building and personal property. Replacement cards may be issued if deemed appropriate by the Department of Campus Police and the Card Authorizer involved. In such cases, a fee per lost card will be assessed by the Department of Campus Police which can be paid by the card holder who lost the card, or by the department if approved by the Card Authorizer. No departmental charges will be made without the Card Authorizer's knowledge.

Upon termination of employment, all cards issued to a card holder must be returned to the Campus Police. It is important for card holders to understand that returning their cards to their department, to the Card Authorizer for their area, or to anyone else other than the Campus Police does not satisfy this requirement.

Primary responsibility for the security of campus buildings, the issuance of key cards, and record keeping rests with the Department of Campus Police. Primary responsibility for the installation and maintenance of locks, manual and electronic lock hardware, and other access control components rests within the Facilities Management Department. Other departments involved in working with the access control system include the Communications Center, Information Technology, Residence Life, and Conference and Events.

## Administrative Card Holders

**A**cademic and administrative buildings of Stonehill College are available for general use by college employees and students for educational purposes. During scheduled hours, the buildings are open (doors unlocked) for classes, meetings and other activities as required. After the normal hours of operation, access to the buildings can be made with the use of a keycard or by calling the Department of Campus Police at (508) 565-5555.

Students who require afterhour's access to academic and or administrative areas must receive authorization from the appropriate Keycard Authorizer. Access to labs will be coordinated with the Department heads. Requests for access to rooms must also be approved by the Keycard Authorizer being responsible for the room for which the access is requested. Access will be issued for up to one semester at a time on the authorization of the appropriate Keycard Authorizer. The individual student accepts the liability for access upon issuance. The student and the department requesting issuance are personally responsible for all issued access until deactivated by the Department of Campus Police.

### Keycard Override Protocol

Keycard override can be used to access electronically controlled doors only during emergencies or exigent circumstances.

The authorized College override key holders are:

- The Department of Campus Police (supervisors only)
- The Department of Facilities Management (supervisors only)

Additional override keys are located in Knox boxes outside of the residence halls for emergency use only by the Town of Easton Emergency personnel.

### Vendor Access

Allowing access to vendors and contractors may be necessary at times; however, this access must be carefully considered. Non-college personnel who have a well defined and ongoing need for access to college facilities may request cards for access to certain areas through project managers who contract for these services. Project managers should contact the Department of Campus Police to arrange for these cards to be issued to approved vendors and contractors. Non-College personnel operating in such capacities will be provided the minimum level and duration of access required for accomplishing their work. Such vendors will be required to return any temporary access cards to the department from which they were obtained prior to departing the campus.

Under certain circumstances, issuance of access cards for specific locations under renovations or construction may be approved for the duration of the project. Access may be restricted to specific locations and granted for a period of days, weeks, or months, and should automatically expire at the end of the stated period.

In cases where there is no ongoing continuous need for access to the facilities, contractors and vendors will either gain access with the assistance of the Department of Campus Police, or obtain access from their project manager. The project manager responsible for the contractor or vendor must submit prior notification of access to any and all department heads responsible for the space.

Access cards will be issued to individuals and these individuals will be held responsible and accountable for all such cards. Cards issued to the contractor or vendor shall not be used by anyone other than the person who has been approved to check them out. All individuals issued cards will be required to sign for their cards. It is the responsibility of both The Department of Campus Police as well as the project manager to maintain records and assure proper usage of each card provided.

The Department of Campus Police will periodically review access card privileges and issuance records to assure security. The Stonehill College Police Department may periodically audit individual and/or departmental card access inventories and records to ensure that there is adherence to these guidelines.

Failure to return cards may result in the contractor or vendor being charged $50.00 for each card. Final payment for work performed or services received is contingent upon compliance with all requirements of this policy.

*It is the responsibility of the project manager who contracts for these services to advise contractors and vendors of this policy prior to the commencement of services.*

**Lockouts**

In case of lockouts, the Department of Campus Police will be contacted. A police officer will respond with a keycard, identify the person requesting access, and then allow access for the authorized individual.

**Nuisance Alarms**

The Department of Campus Police will maintain an active follow up procedure for nuisance alarms as well as working with the appropriate departments to resolve repetitive alarms. When a nuisance alarm becomes significant, The Department of Campus Police with the approval of the Shift Supervisor reserves the right to reduce or eliminate the alarm temporarily. The individual silencing the alarm will be responsible to notify all appropriate parties (Residence Life, Communications Center, IT, Facilities Management, Card Authorizers responsible for that space, etc.), and must submit a work order for any necessary repairs.

**Access Violations and Alarms**

The following are examples of violations of the Access Control Protocols:

Loaning keycards
Transfer of keycards without authorization
Altering locks or mechanisms
Damaging, tampering or vandalizing any Stonehill College lock, hardware or system component
Unauthorized propping open secure doors
Admitting unauthorized person(s) into a building
Failure to return a keycard when requested by The Department of Campus Police, or upon leaving the employment of the college
Failure to report missing keycard(s)

The Department of Campus Police and the Communications Center have the responsibility of monitoring alarm activity and responding appropriately by either dispatching a The Department of Campus Police Officer or notifying the appropriate personnel of alarm activations.

Held Open Door Alarm

These alarms are generated after any monitored door is held open longer than the configured period of time. After this alarm has been triggered, an event will be generated in the system, and an audible local alarm will sound at the door until the door is closed. If an alarm continues to sound for a considerable period of time and a designated staff member is not available to respond, a police officer should be dispatched.

## Lost Card Replacement

Lost, stolen or damaged keycards must be immediately reported to the Department of Campus Police. Campus Police will deactivate the lost, stolen or damaged keycard and produce a replacement card for the cardholder. Individuals may call Campus Police at (508)565-5555 with any questions.

Before an individual will be issued a replacement keycard, this individual must present valid photo identification. The person issuing the new card must create an entry in the Police log which includes the following information:

- What type of ID was shown
- Name
- Stonehill ID number
- Lost or cancelled card number
- Reason card was cancelled

**Person:** John Doe
**Proof of Identification:** Massachusetts Drivers License S 123456789 Expiring 10/1/07
**Stonehill ID:** 123456
**Lost or cancelled card number:** 02468
Card was lost on January 1, 2007

Until individuals report the card lost or stolen, they are responsible for any activity on this card, including loss of funds. After it is reported, the card will be deactivated and unusable.

A replacement fee of a $50 per card must be paid prior to receiving a replacement card. If the access card is later found it must be returned to Campus Police. Replacement(s) will not be issued until the report has been cleared by Campus Police and all charges have been paid.

## Unlocking/Locking Doors

In the event there is a need to deactivate the locking mechanisms, only the Director of Campus Police or designee has the authority to approve this request. When this feature has been deactivated, the person deactivating the feature must log an entry into the monitoring client, indicating who requested this procedure, the reason for the request and who authorized the request.

### Disabling System Features

Under specific circumstances, system features can be disabled at the discretion of the Director of  Campus Police, or his/her designee.  This feature, however, must be carefully considered. When a feature has been disabled, the person disabling the feature must log an entry into the monitoring client, indicating who requested this procedure, the reason for the request, and who authorized the request.

Project managers who are overseeing projects which may need this feature disabled should contact the Department of Campus Police to arrange for these area to be disabled. This feature will only be provided under specific circumstances, and for the minimum duration required for accomplishing their work.

### Academic/Administrative Areas

Designated perimeter doors may be outfitted with access control system components. Access groups for these areas will be determined by location and will correspond to the dates/times that the buildings are open.  The Director or designee will also oversee all occupancy changes as they occur throughout the year.

### Privacy Issues

- The Access Control and Security System is not a time-and-attendance system, neither is the system a device for monitoring traffic of students, faculty and staff.
- The system does, however, produce and retain information for a pre-defined typical period (for example a full semester) of access activity.  After this period, the activity is either archived for necessary investigative purposes or discarded and overwritten.
- Limited archival of activity may be needed for crime investigation purposes and investigations.
- The system typically does not monitor exits from doors; however, exceptions can be made for high security areas.
- The Vice President for Student Affairs and the Director of The Campus Police, or their designees, have the authority to authorize reports associated with criminal investigations.  No personnel requests on “time-and-attendance” issues should be produced unless they relate to investigations.
- College policies and FERPA are observed by all functions of the access system.

### College Closing

During semester breaks in which the College is closed, access to buildings may be deactivated unless prior approval is granted by the Card Authorizer.