

# VCU INTEGRATED ACCESS CONTROL POLICY



VCU POLICE DEPARTMENT

## **FACILITY ACCESS GUIDELINES AND PROCEDURES**

### **Purpose**

Virginia Commonwealth University is committed to the safety and security of all members of its community by maintaining the security of its facilities and physical environs. While the University will endeavor to maximize control of access to buildings and other facilities, it is ultimately the responsibility of each unit or department to determine the mechanism used, determine who is entitled to request and obtain access to their respective areas and submit appropriate approvals to the VCU Police Access Control Division.

### **Policy**

To establish a systematic method for procuring and maintaining door keys and building access cards (VCU One Card).

To provide the University's guideline for the purchase and maintenance of locking systems.

To maintain quality mechanical and electronic standards for security and crime prevention on campus.

This policy governs all locking devices used on any property owned or leased by VCU.

### **Procedure**

#### *Locking Mechanisms*

- Facilities may be secured using two types of technology:

*Mechanical Lock:* This consists of the utilization of keys or punch locks that have the function of opening doors.

*Electronic Access Control:* This consists of the utilization of systems that report to either a local or remote processor for documentation of entrance. Typically, this would include keypads or card readers, or a combination of both, activated by the One Card.

- All lock requests must be authorized according to the guidelines and procedures listed below.
- Authorization requirements vary according to the requested level of access.
- Authorization requirements vary according to the access level of the key for mechanical locks.

### **Mechanical Lock & Key Guidelines**

### *Master Key System*

All door keys must be acquired according to the established procedure and manufactured through VCU Facilities Management Division. The Master Door Key system shall be maintained within all university buildings. Departments desiring removal from the Master Key system must have prior administrative approval. Each department or their designee head is responsible for all the door keys issued for their department.

- On the Academic Campus, campus-master or grand master keys require a signature of the Provost or Vice President. Below the level of master key, authorization is required by the appropriate administrator (dean, Department Head, Program Director, etc.) for their respective buildings or areas.
- For the MCV Campus academic facilities, campus-master, grand master, building-master, floor-master, wing-master, crosswalk-master, tunnel-master and off-master keys require the signature of the Vice President for Health Sciences or his designee. Authorization for all other keys must be from the appropriate administrator (Dean, Department Chair, Program Director, etc.).
- The Physical Plant Locksmith should be notified in writing (P.O. Box 980246) of any special departmental restrictions.
- University key requests must be submitted on a signed requisition or memo with appropriate level signatures. Signature definition: Department Head or department Head's approved designee as recorded on the Authorized Signature Cards which are maintained in Materials Management Department.

### *Duplication of Door Keys*

- Complete a VCU Purchase Requisition ensuring that the following information is provided:
  - ⇒ Department Name
  - ⇒ Department Account Code
  - ⇒ Building, floor and room number of requested keys
  - ⇒ Number of keys required for each door
  - ⇒ Signature of Department Head or his/her authorized designee as stated on the department's Authorized Signature Card on file in Materials Management
- Deliver the requisition to the . The requisition shall be signed by the department director or their designee and recorded in the Engineering Requisition File. FAX (828-9128) or mail (P.O. Box 980279) the requisition or memo to the Physical Plant Service Center.
- Be sure to include key code number, if available, and specify location where the key is to be used.
- After receipt of the signed requisition or memo, the Physical Plant Service Center shall verify authorization level and issue a work order ticket to the University Locksmith noting

the approval level received. The signed requisition or memo shall be filed for future reference if needed.

- The Locksmith shall check the code file for any special departmental restrictions.
- The average charge with no extraordinary circumstances is \$2.00 per key, plus delivery.

### *Special Order Locks*

- Departments with special order locks must follow the established authorization procedures for keys or combination changes. Service to special order locks (exterior or interior) shall also be charged to the requesting department.

## **Electronic Access Control Guidelines**

### *Access Authorization*

- The individual user will obtain a One Card from the VCU One Card offices located in the libraries on the academic and medical campuses. Pertinent information will be automatically downloaded into the access control host computer at the VCU Police Department.
- To activate or upgrade a user's access to a particular building and door, the card user must do the following:
  - ⇒ Request access from the immediate supervisor for all areas needed. If the supervisor grants approval, the Access Request Form must be completed. (See "Individual Access Request Form Guidelines"). The form shall be forwarded to the next level as outlined below:
    - \* **Academic Campus**: the appropriate administrator (Dean, Department Chair, Program Director, Building Manager, etc.) must authorize Electronic card access for a specific facility or space. This authority must be conveyed to VCU Police Access Control Division with name and VCU One Card Number.
    - \* **MCV Campus academic buildings**: the appropriate administrator (Chairman or Director, Dean or Building Coordinator, etc.) must authorize electronic card access for a specific facility or space. This authority must be conveyed with the name, Social Security Number and One Card Number to the Office of the Vice President of Health Sciences (VPHS). When the request has been approved, VPHS will forward it to the Campus Police for activation. \*\* If your request does NOT include any MCV Campus academic facility or animal facility, you may submit the request directly to the Campus Police Department after being signed by the appropriate building coordinator..
    - \* **MCV Hospital Facilities**: MCV Hospital must authorize electronic card access. This authority must be conveyed to the MCV Hospital Security Division. It must include the name, SSN and One Card Number of the cardholder, the door(s) needing access through and area(s) of access.

- \* **Animal Facilities**: the Department of Animal Resources must authorize electronic card access.

### *Individual Access Request Form Guidelines*

- To request that building access be activated for a student or employee's One Card, complete the top portion of the Access Control Request Form.
- Be sure to indicate which building and which doors the individual should be allowed to access.
- Upon receiving access approval, the cardholder shall be authorized access to established card reader doors at the approved times. Cardholders shall check with the Building Coordinator to determine what access they are assigned. The Building Authority with the VCU Police Access Control Division shall determine the access level to which individuals are assigned.

### *Deactivation of Card Access*

- The Building Authority shall notify the VCUPD immediately when anyone needs to have access authorization deleted. The Building Authority shall also conduct monthly reviews of their access authorization list and report any changes to the Office of A.C. To request that the building access for an individual's card be deactivated, complete the top portion of the Access Control Request form, with the appropriate Dean's signature in the DEACTIVATION ONLY section. These must be submitted in a timely manner.

### *Lost Cards / Replacement Cards*

- After a replacement card is issued, complete the top portion of the Access Control Request form with the new card information and re-submit the request to the Police Department. You are NOT required to send the request through VPHS if you are requesting activation of a replacement card for an individual who was previously given access.

### *Schedule Change Request*

- This section of the form is used by Building Authority to request changes in the locking schedule of doors and buildings.
- Schedule changes for MCV Campus academic facilities shall be submitted to VPHS for approval before they are forwarded to the Police Department.
- Schedule changes for other buildings may be submitted directly to the Police Department as long as the appropriate Dean's signature is included on the form.

### *Submission*

- Approved request forms shall be submitted directly to the VCU Police Department Access Control Division, Box 842024, or fax to 828-1199.

- ⇒ Vice President for Health Sciences- Box 980549, fax 828-8003. E-Mail is accepted.
- ⇒ MCV Hospital Security- AD Williams B-503, Box 980320 fax 828-4299.
- ⇒ Department of Animal Resources- Sanger Hall B1-052, Box 980630, fax 828-2705.

### *Activation Status*

- The VCU Police Department, Office of Access Control, requires 48 hours notice prior to making changes. It is highly recommended that requests for activation for weekend or holiday access be submitted as early as possible. To check on the status of a request, contact Access Control Division at 828-9373, or email [swkelley@hsc.vcu.edu](mailto:swkelley@hsc.vcu.edu)
  - ⇒ This authorization and entry process may take a few days. If authorization was approved, and the card is not permitting access, check the lights of the reader to help determine the reason for denial. If the reader is flashing yellow, your card is not being read. This means you need to contact the VCU One Card office. If the card reader is flashing red, check with your supervisor to verify that your authorization was approved.
- When Card holders need to gain additional time or card reader access, the following shall be done:
  - ⇒ Notify the Building Authority to determine need;
  - ⇒ If granted, fill out the Individual Access Request Form;
  - ⇒ The appropriate administration will review and forward completed forms to:

VCU Police  
Access Control Division  
PO Box 842024  
FAX: 828-1199

## **Installation and System Operating Standards**

### *Perimeter*

- The perimeter of each facility shall be identified and controlled by the VCU Police Integrated Access Control System (IACS) and Emergency Communication Center.
- The main points of access into facilities shall be controlled using card reader technologies that will read the VCU One Card I.D. A PIN keypad will be included with most card readers.
- A hands-free telephone should be installed with these card readers at the entrances to most buildings. These phones shall communicate with VCU Police Emergency Communications Center to assist with customer service for after hours, when a building is secure. When internal visitor control is required, a tenant directory should be included with the phone.
- All designated emergency egress doors, which open on ground level, shall be controlled using time delay magnetic locks with a 30-second delay.
- Loading dock doors shall be controlled from both the entry and the egress side using magnetic card stripe readers (i.e. in/out card readers).
- All perimeter doors shall also have door alarm magnetic contacts. The contacts shall be recessed wherever possible, or armored.
- Approved magnetic locks and or electric strike locks shall be installed on the doors to be controlled by card readers.

### *Internal Controls*

- Any room or sensitive area that needs control shall be identified by the end-user.
- Identified internal controls may be integrated into the system, approved and monitored by VCU Police.
- Elevators: All new elevator installations should include wire roughed-in for the potential installation of card readers to control the use of the elevators after hours. The required cable is 3-pair, stranded, individually shielded, with an overall shield, 22AWG, Plenum rated cable. This cable should be included with the 'traveler' cable in the elevator shaft. The cable should be terminated in the elevator machine room.

### *General Installation*

- IACS data gathering panels shall be included with a 4-hour battery backup, power supply. The panels will need to be installed in a secure telecommunications riser.

- All cable shall be concealed inside the wall or ceiling and marked appropriately. Conduit shall be provided when it is not possible to conceal or protect the cable.
- All cable will be Plenum rated.
- All locks, readers, etc. shall be integrated into the building fire alarm system so that if an alarm/fire should occur, all locks shall immediately fail-safe open.
- The building systems shall be connected back to VCU Police Emergency Communications Center using leased line telephone modems until a fiber optic network has been completed. VCU will have to provide the required leased telephone line.
- Telecommunications shall authorize the installation of the phone lines. All phone lines shall be Centrex lines and shall terminate on an RJ11C jack in the primary location. This line will be used as a modem line for the IACS. The lines should have access to long distance calling via the authorization code feature, call screening but deny access to third party billing.

### *Planning and Development*

- VCU Police Crime Prevention Division and Access Control staffs, a qualified vendor (Security Technologies Group) and the VCU Facilities Management Division shall be involved in the pre-planning stages of design and planning.
- Provide building plans in a CAD file on disk to security vendor.
- Security vendor shall work with VCU to develop system design and budget.
- Security vendor shall work with VCU Police Access Control Project Manager to coordinate work that should involve other trades such as door hardware, conduit, and power requirements, etc.
- Security vendor shall create construction documents inclusive of door details, conduit and power requirements, wiring riser diagrams, and system component location charts to be included in the review package that may go to the state and any bid documents that may go out to the general contractors.
- Security vendor shall make all necessary presentations to the Fire Marshall concerning the system design.
- Security vendor shall provide a formal submittal to the Project Manager once the purchase order has been received. Submittal will include all project documentation, prints, risers, installation schedule, quality control plan, and system acceptance testing procedure/plan.
- Once the project begins, the security vendor shall provide all project management and engineering required to support the project.
- Security vendor shall provide a total turnkey project.

- Security vendor shall provide as-built drawings to VCU when the project has been completed, and is CAD drawings were provided.
- The Manager of the Office of Access Control will be responsible for managing the contracts of all vendors (Contract Administrator). This shall be done with the assistance of the Contract Administrative Assistance Program form.

### *Fire Alarm Panels*

- When a new site is installed, the security vendor shall notify the Access Control staff. The Access Control staff will set up an appointment with the Zone Maintenance Group or Fire Panel Contractor and the security vendor to connect the IACS panel to the fire panel. This connection is necessary to ensure that when the fire alarm is pulled all electronically controlled doors are automatically unlocked.
- All doors designated as emergency exits shall have free or delayed egress. These doors shall be integrated into the building fire system.
- Each door shall meet the current State of Virginia Fire Code and Life Safety standards. Safety inspections of doors shall be conducted by the Office of Fire and Occupational Safety
- The following sign must be placed on each emergency exit door:  
**‘Push until alarm sounds. Door can be opened in 30 seconds’**
- All signs must contrast with the actual doors. The color scheme is usually orange lettering on a transparent sticker.

### *VCUCard*

- A. The VCUCard Office is responsible for issuing the cards for access control. Magnetic swipe cards are issued to all users and dual tech (proximity) cards are issued to all students and staff who need access into buildings using the proximity readers. VCUCard issues the cards to the user, then the information is downloaded to the VCU A.C. Server. The VCUPD is responsible for granting the access to the cardholder after receiving an authorization from the proper building authority.
- B. VCUCard Office is responsible for supplying the VCUPD Access Control Server with current student, faculty, staff and contractor information. This is done through continuous downloads. Currently downloads occur every 5 minutes from 7am-10pm each workday. They also occur at midnight of each day.
- C. The Cardholder Application Analyst (CHAA) of the VCUCard Office monitors the VCUPD updates. The CHAA receives alerts whenever the VCUPD’s server does not receive data. The CHAA will notify the VCUPD AC Programmer when there is a problem with the downloading process. In the event that VCUPD discovers the data is not properly downloading, the AC programmer will contact the CHAA through the online service center

at <http://beech.vcu.edu/das/homepage.nsf/CSFrameset?openframeset> or call the Help Desk at 828-1802 or e-mail them at [dashelp@vcu.edu](mailto:dashelp@vcu.edu) . If it is an emergency, the programmer may call directly to the VCUCard Business Manager (Patti Murdock). They will follow the following guidelines to resolve the problem:

1. Contact Security Technology Groups to assist with problem resolution.
2. Contact VCUPD AC Manager of status of problem.
3. Contact Director of Education if a resolution can not be resolved immediately.
4. Contact any building manager or coordinator who may be effected when data update is not completed (e.g. each housing office).

D. It is important for the VCUPD and VCUCard Office to thoroughly troubleshoot all customers' card issues before contacting or referring the customer to the other department. The VCUPD will run through the following checklist when a card is not working on a specific card reader:

1. Determine if the cardholder was given a clearance on the door in question. Be certain that the cardholder explained the correct door.
2. Determine if the cardholder is currently enrolled in school (if they were not enrolled for the previous semester, their card may be on the inactive list). They must enroll to activate their card.
3. Determine what the color on the reader indicated when the card was swiped. Green means the card worked and granted access. Red means the card worked but is not granted access. Yellow means the card was not read at all, which indicates the card may need to be replaced.
4. Determine if there were reader problems. If the problem was from the reader, have the customer test their card at the reader again (if convenient) or test at a nearby reader. Some potential reasons for the cards to be rejected are:
  - a) Reader is not functioning properly or needs to be cleaned.
  - b) Card is not swiped properly.
  - c) Reader/door was not reset/closed and lights were flashing.
  - d) The security panel at the building had not been currently updated at the time of the swipe, therefore it would take 30-50 seconds for the reader to query the main server and grant access.
5. During the first two weeks of school, contact the VCUCard Business Manager at 827-1660 when there may be a problem with the card itself.
6. During all other times, contact the VCUCard Office at 828-8385.
7. If they are not in the system, contact the VCUCard Office through the online service at <http://www.vcu.edu/vcucard> .

E. The Office of A.C. and VCUCard Office shall notify each other in the event of any issues that may effect the other department. This shall include when a new building is going to use proximity card readers, when there are any modifications in the cards or readers or when there are any changes in procedures.

- F. Contractor issued cards will be issued by the VCUCard Office. They will contain an expiration date to ensure proper deletions from the system. The B.A. is responsible for collecting the cards from the contractors upon completion of their jobs or termination of contracts/employees.

### *Inclement Weather Procedures*

#### A. NOTIFICATION

1. Any member of the VCUPD who is officially notified of the inclement weather closings will immediately notify the Emergency Communication Center (ECC). When the ECC is notified, the ECC Dispatcher will confirm the closing by calling the inclement weather number (278-1727). The following personnel will be contacted by ECC in the following order:
  - a) Access Control Programmer
  - b) Patrol Commander
  - c) On-duty Security Supervisor
  - d) Deputy Chief of Support Services
  - e) Security Manager
  - f) Access Control Manager

#### B. LOCKING RESPONSIBILITY

1. The Access Control Programmer will be notified of the inclement weather closing times. The programmer will immediately cancel unlocking commands for all buildings. The order of the buildings will be according to a pre-determined priority list. This list should prioritize the buildings according to the scheduled unlocking times.
2. The Access Control Manager and Programmer will be responsible for providing and updating the Access Control Inclement Weather Building lists. They will each maintain a copy of the Access Control Inclement Weather Building list. A copy will also be posted in the ECC Standard Operating Procedures manual and Access Control manual.
3. The Access Control Programmer will schedule each building to lock down until 15 minutes prior to the predetermined opening times. The programmer will notify the ECC once all buildings are secure. The ECC Dispatcher at the access control station will be responsible for ensuring that the buildings unlock at the new scheduled times.

#### C. EARLY UNLOCKING REQUESTS

1. ECC will honor requests from listed building managers/coordinators to unlock their buildings early. These unlocking requests will be handled at the actual time the request is made. No requests will be delayed or scheduled to be unlocked at future times. The building managers/coordinators will provide the ECC with the actual door(s) or door group(s) to be unlocked.

#### D. POSTING PROCEDURES

1. A copy of this directive will be placed in the ECC Standard Operating Procedures manual and the Access Control manual. The Lieutenant of Education and Training, the Access Control Manager and the ECC Manager will review this directive October of each year. The ECC Manager will be responsible for distributing this directive to all ECC staff after each review. Each manager/coordinator for electronically controlled buildings will be given a copy of the directive.

### *Maintenance and Invoice Processing*

The VCUPD A.C. Manager shall receive training in Contract Administration (CA). The CA is responsible for monitoring and management of all maintenance/service work to electronic security systems. This work shall include the maintenance of doors that are controlled or monitored by VCUPD electronic security equipment. The CA shall approve all work completed by vendors, contractors and VCU maintenance workers. All invoices shall be reviewed and approved by the CA.

### Placing Service Calls

Building Authorities shall route all service calls through the VCUPD Emergency Communication Center at 828-1196 .

The ECC officers shall record the service request in the VCUPD Maintenance log manual, located at the VCUPD ECC.

ECC officer shall assist the caller in troubleshooting the problem in order to confirm an actual need for maintenance.

When there is uncertainty as to the necessity of a service call, ECC shall have a trained person (police officer, security guard or building authority) check on the problem.

When it is still uncertain, they shall contact the A.C. manager or programmer during business hours.

The ECC officer will determine where the maintenance call shall be placed based on the following criterion:

Security Technology Groups- Only problems with their electronic equipment.

Customer Service Center- for door closure problems or non electronic failures.

Housing office- all non-electronic (STG) equipment failures, eg. door closure.

Student Commons- all non-electronic (STG) equipment failures, eg. door

closure.

Hospital Security- For all repairs needed to all Hospital equipment.

Stoney Point-

After hour problems shall always be assessed by an officer. The officer shall report to the patrol commander any repairs that need immediate service. If the officer feels the problem needs to be resolved immediately, need to be approved

VCUPD will store particular parts at their Property Office. This will prevent long ordering process of unavailable parts or prevent the vendor from having to return to their office to get

parts. These parts will be inventoried yearly. The authorized Property Officers will fill out a sign in/out sheet when parts are turned in or signed out by the vendor. The Property Office will notify the A.C. Manager whenever parts are checked out. The A.C manager will reconcile the usage of the parts on the vendor work order and make sure the VCUPD is not being billed for their own equipment.

## **ELECTRONIC SECURITY USER AGREEMENT**

### *1. Purpose*

- 1.1. The purpose of the “Electronic Security User Agreement” is to outline the responsibilities of the Virginia Commonwealth University Police Department and the University departments that use electronic security systems. It establishes a comprehensive and standardized means to regulate and finance security systems throughout the University. The security system user enters into a partnership with the VCU Police Department. These partners will work together in assessment, design, installation and management of the security systems. Through standardization and cooperation the user will have the appropriate system which will be compatible with the University mission of enhanced safety, security and crime prevention at VCU.
- 1.2. It shall be mandatory for any department that uses an electronic security system, which requires an alert of and a response by members of the VCU Police Department, to enter into this user agreement.
- 1.3. This agreement establishes a system of administration, drafts procedures and regulations, sets a fee schedule for police services (after installation) and outlines disciplinary recourse for violations.

### *2. Responsibilities of the VCU Police Department*

#### 2.1. Establishment of Policies and Procedures

- 2.1.1 The VCU Police Chief will establish guidelines and procedures that govern the management and operations of the Access Control System and the response of Police Department members and resources.

#### 2.2. Recommendations for Access Control System

- 2.2.1 The VCU Police Crime Prevention Division will be responsible for the recommendations and approvals of all field device(s)
  - A. Recommendations of field device(s)
    - a) The VCU Police Crime Prevention Division will specify appropriate security devices that will meet the needs of the alarm user and be compatible to the VCU Police monitoring station. Crime Prevention will conduct a security analysis and gives recommendation to the appropriate building authority.
    - b) The recommendations shall be consistent with the standards outlined under ‘*Installation and System Operating Standards for the Access Control and Security Management System of Virginia Commonwealth University*’ and ‘*Facility Access Guidelines and Procedures*’.
    - c) Crime Prevention Staff must be represented on any committee where physical security and integrated system issues are addressed.

## B. Approval of Field Device(s)

- a) The Building Authority shall submit floor plans or blueprints (preferably in 8 1/2 X 11 and C.A.D.) to Crime Prevention for their review. Crime Prevention shall recommend and approve the design of any security system at any university facility.
- b) The Chief of Police will have final approval of all security plans. Denial of any security system can be appealed to the Chief of Police.
- c) Certain audible alarms will be prohibited. It shall be in violation for any person to sell, lease or install, and for any alarm user to purchase and maintain, upon any Campus premises, an audible security alarm system designed to be heard outside of the premises, which emits a sound that resembles the signal commonly made by a police or emergency vehicle. In addition, any audible alarm system used on the VCU Campus must be designed to automatically shut off after sounding for a maximum period of fifteen minutes. Audible alarms will be prohibited unless there is a means for VCU Police Emergency Communication Center to receive the security alarm signal.
- d) All systems will meet current standards set forth by State Fire Codes. Systems will meet approval of Fire Safety of the Office of Environmental Health and Safety.

## 2.3. Training of System Users

2.3.1 The VCU Police Department or designated vendor shall conduct the necessary training for the building authority, staff members and/or students. A New Users Training Package shall be given to Building Authorities before turning a building on. Training will consist of:

- A. system management
- B. maintenance requirements
- C. door and user groups
- D. scheduling
- E. purpose and usage of card readers
- F. troubleshooting door and card reader alarms or problems
- G. initial staff training

## 2.4. Monitoring Access Control and Alarms

2.4.1 The VCU Police Emergency Communication Center shall be responsible for monitoring all approved alarm systems. All approved alarm points will be received in the Emergency Communication Center. The dispatchers shall;

- A. monitor system and incoming alarms,
- B. dispatch VCU Police Officers to investigate alarms or system malfunctions,
- C. log maintenance reports as received from the responding officers,

- D. re-set alarm points and doors,
- E. notify Access Control management when malfunctions occur which are either unusual or appear to need special attention,
- F. report immediate maintenance requests to Security Technologies Group Service Center (or designated vendor).

2.4.2 The VCU Police Emergency Communications Center shall establish specifications of appropriate signaling devices that will be compatible with their operation. The Building Authorities must comply with requirements of the Emergency Communications Center.

2.4.3 It shall be a violation for any person to install, sell, lease, or use an automatic telephone dialing device or system which is set or programmed to directly dial, call, or in any way make direct contact with any telephone line or radio circuit of the VCU Police Emergency Communications Center without prior approval.

2.4.4 Dialer Alarms compatible with the VCU Police Emergency Communication Center's monitoring panel are subject to approval by the Office of Access Control.

## 2.5. Response and Investigation of Alarms

2.5.1 The Patrol Division of the VCU Police Department shall be responsible for responding to alarm calls. Officers shall respond to the location of the alarm and investigate as to the nature or cause of the alarm. Once the cause of the alarm is determined the officer shall take appropriate action.

- A. Search the area for intruders
- B. Secure the door(s)
- C. Notify E.C.C. of any defects (E.C.C. will call in any work order)
- D. Notify staff of proper procedures
- E. Assist staff
- F. Notify Access Control of violations of IACS policies, procedures or physical security deficiencies.

## 3. *Responsibilities of the Building Authority (Manager/Coordinator)*

### 3.1. Agreements

3.1.1 The Building Authority shall have on file a copy of the Electronic Security User Agreement. That individual's responsibility is to assist, promote and abide by this chapter. The Building Authority shall submit any changes in writing, on the appropriate forms to the Police.

3.1.2 Any Building Authority who operates or allows a security system to be operated without prior approval by VCU Police shall be in violation of this agreement.

### 3.2. Notification of Alarm Business

3.2.1 The Building Authority shall notify any and all alarm businesses of the requirements outlined in this agreement.

### 3.3. Registration

3.3.1 Every Building Authority of any approved system other than the VCU Police IACS shall submit a written request to the Chief of Police for the operation of such security system. The person applying for registration, required in this section, shall state the following:

- A. Name and address of the commercial or residential premises in which the system will be installed; telephone number of the alarm user; the type of security system; and who will be monitoring the system;
- B. Name of the security alarm business selling or leasing the new or existing alarm system equipment or services.

3.3.2 Names, addresses, and telephone numbers of at least two contact persons. These individuals will be called at any time, day or night. They must be authorized to respond to an alarm signal and be able to open and represent the premises in which the system is installed, for reporting and investigative purposes.

3.3.3 It shall be the responsibility of the Building Authority to notify the VCU Police in writing of any subsequent changes in the information provided on the registration application. The application registration is subject to review by Crime Prevention and Access Control, and to the approval by the Chief of Police.

3.3.4 No alarm system shall be installed, monitored, altered, serviced or repaired to a level of operation by an alarm business unless the Building Authority has complied with the registration provisions of this agreement.

### 3.4. Maintenance

3.4.1 The Building Authority shall be responsible for maintaining the security system in working order, free from false alarms. This will also include maintenance of doors and associated hardware. Continuous alarms due to maintenance may result in a fine (See Resolution of Security System Issues).

### 3.5. Training and Supervision

3.5.1 The Building Authority shall instruct employees, tenants or others, who may have occasion to activate an alarm, that security systems are to be activated only in emergency situations to summon an immediate police response. They shall also instruct as to the operation of the alarm system, including setting, activation, deactivation, and resetting of alarms. All instructions pertaining to security systems and procedures shall be in written form, suitable for distribution, and shall be available for review by representatives of the VCU Police Department.

3.5.2 The Building Authority or their designee shall submit a written request to the Office of Access Control for any Access Reports for their buildings. These reports shall be generated and distributed within two (2) working days.

### 3.6. Scheduling and User Groups

3.6.1 Access control is a crime prevention method whereby occupants of a building are directed to only use specified entrances and exits at any given time. An Access Control System means basically that the building will now be locked and unlocked electronically by a computer turning on or off magnetic locking devices instead of using a person with a key. The Building Authority plays a critical role in the success of an Access Control System by determining when their building will be secured and who can gain access after hours. When a building is locked, occupants who have been authorized can enter a building using a card key versus a mechanical key. A computer record is generated each time an alarm is generated, a card is swiped through a reader, or some other action is taken in the system.

3.6.2 The Building Authority shall specifically define and restrict access hours and groups. The Building Authority shall designate a building liaison who shall communicate between the building occupants and the VCU Police Department Access Control staff. The liaison shall determine how the Access Control System will be operated according to the building and division's unique needs. The VCU Police Access Control staff shall work with them on determining how to program the database to operate for each building. This is done in three ways.

#### A. ***DETERMINE SCHEDULES***

- a) When should the building be unlocked for business?
- b) What doors should be unlocked at this time?
- c) Are there any doors that should be locked 24 hours a day?
- d) Consider fire exit doors, interior doors versus exterior doors.
- e) Card Reader Door schedules
- f) Provide a written list of all schedules, including building name, door numbers, days of the week, weekends and don't forget to provide a HOLIDAY SCHEDULE.
- g) This list should include the authorizing person's name, department name and phone numbers and signature. This person should be a Vice President, Dean or his/her designee.

#### B. ***DETERMINE CARD AUTHORIZATION RECORDS***

- a) WHO is allowed in the building after regular working hours when the doors are locked?
  - Consider special populations, i.e. Only faculty are allowed in some doors; or Housekeeping, Facility Management workers, etc.
- b) Obtain this information from authorized persons:
  - FULL NAME,
  - SOCIAL SECURITY NUMBER,

- VCU ONE CARD NUMBER.

⇒ Note: A list will not be accepted for data entry without ALL three of these elements of information.

- c) Document this information along with which building.

### C. **AUTHORIZATION DOCUMENTS**

- a) Provide a letter from the department head authorizing a designee in the building to authorize card access lists, scheduling and any changes.
- b) Provide a list of AFTER HOURS Contact Information on who should be called if a major incident should occur after hours. This list should be of home telephone numbers.

3.6.3 The Building Authority shall produce timely employment updates for activation and removal of employee access to the Office of Access Control and when necessary to the VCUCard Office. The Building Authority shall notify the VCUPD immediately when anyone needs to have access authorization deleted. The Building Authority shall also conduct monthly reviews of their access authorization list and report any changes to the Office of A.C. VCUPD shall conduct periodic reviews of this process to ensure that all lists are being updated expeditiously. Departments that do not keep the list updated shall be notified of the infraction. A second offense shall be reported to the Office of the Senior Vice President for Finance and Administration.

3.6.4 The Building Authority shall submit any access requests 48 hours prior to needed changes. The Access Control manager will promptly notify the Building Authority of the first violation of this directive. All violations after the second shall result in a fine (See Resolution of Security System Issues).

3.6.5 All doors shall be placed into categories call ‘Door Groups’. The VCU Police AC staff will provide a door group list to the VCU Police Emergency Communication Center and the Building Authority.

### 3.7. Deliberate False Alarms

3.7.1 Any person who intentionally or deliberately, and without just cause, activates an alarm system in a non-emergency situation shall be deemed in violation of this chapter and 18.2-461 Code of Virginia (Falsely summoning Law Enforcement Officials- class 1 misdemeanor). Nothing herein contained shall apply to the periodic testing of alarms after prior coordination with and approval of the VCU Police Emergency Communications Center. Testing the alarm systems without such prior coordination and approval is in violation of this section (See Resolution of Security System Issues).

## 4. *Resolution of Security System Issues*

- 4.1. It is the intent of the VCU Police to resolve issues in an informal and just fashion. The Manager of the Office of Access Control will immediately contact the Building Authorities of any concerns and will assist them in quickly resolving issues.
- 4.2. For any and all violations or concerns, the following procedure shall be utilized:
  - 4.2.1 Police officials shall contact the Building Authority.
  - 4.2.2 A plan shall be developed to resolve issues.
  - 4.2.3 All costs shall be the responsibility of the Building Authority.
  - 4.2.4 Possible resolutions shall include, educating staff, students and visitors, fixing doors, changing monitoring or alarmed times, changing system design or programming, fining or counseling violators, or removing access of violators.
  - 4.2.5 Violations by students shall be addressed through the established student affairs rules and procedures. Any student who is stopped while working for VCU will be addressed as an employee.
  - 4.2.6 Violations by employees shall be addressed through established Human Resources policies.
  - 4.2.7 All other violations shall be reviewed and resolved by the Building Authority.
- 4.3. The third false alarm originating from any premises and to which police are dispatched or respond within six consecutive months shall result in a service fee being imposed by the Police upon the Building Authority, which must be paid within 30 days after the billing. The service fee shall be twenty-five dollars (\$25.00) for the third false alarm and forty-five dollars (\$45.00) for the fourth false alarm and each subsequent false alarm.
- 4.4. The Police shall notify the Building Authority upon occurrence of the fifth false alarm within a six-month period that the security system must be inspected by a registered security alarm business to identify any problems or defects with the security system. The choice of a security alarm business and cost of the inspection are the responsibility of the Building Authority. The security alarm business shall provide a copy of a report of inspection to the Chief of Police. The report shall outline the problems or defects found and the actions taken or needed to correct such problems or defaults. If no problems or defects are noted, the report must certify the system as operable. If the system is certified operable, it will be presumed that the false alarms occurred through alarm user error. The user must then be retrained and/or provide an alarm operator's training program for its employees, tenants, and all others having access to the system. A report of this training must be filed by the Building Authority with the Chief of Police or his designee.
- 4.5. The final resolution shall be a letter sent to the Building Authority that the Police will not be responding to any security alarms until the issue is resolved. After proven resolution, the VCU Police shall deem the system operative, and shall re-establish monitoring.

4.6. Alarms generated by faulty electronic security equipment will only be considered for penalties when the Building Authority has not taken appropriate actions to correct the problem.

5. *Promulgation of Regulations by Chief of Police*

5.1. The Chief of Police shall have the authority to enact and enforce reasonable rules, rates and operations for this agreement in the interest of public safety, morals and welfare, and to effect the general purpose of this agreement.