A. Policy.

It is the policy of the Department of Public Safety to establish and maintain a Card Access Program as a measure to assist in accomplishing the department's mission. The Card Access program, when used with the other security methods employed by the department, will form an integrated security system, protecting students, facility, personnel and property campus wide.

B. Procedure.

1. Mission

The Card Access program will control access to buildings, floors and rooms on campus. One of the main functions of the system is to create a record of time and dates at which events occurred. Buildings can be opened and locked automatically, securing them during non-business hours. Buildings can also be secured in the event of a campus emergency by activating the emergency lock down system.

2. Duties

a. Systems Administrator

1) Responsible for the day to day operations of the system.

   a) Approve card access requests when they are received

   b) Conduct daily inspection of computer reports to verify
c) Conduct daily operational checks of the card access computer system

1. Making sure the computer will take keystroke commands.
2. Making sure the system is receiving transmissions from the building’s card reader and alarm panels.

d) Program/re-program door opening schedule to meet the needs of clients.

e) Program and define the required card access alarms to ensure proper Public Safety response.

2) Training of personnel

a) Administrative personnel
b) Dispatch personnel

3) Issuing Passwords and security levels for system operators.

4) Coordinate with Department Heads to ensure understanding and compliance with system requirements.

5) Responsible for the Card Access Computer.

a) Software
b) Hardware

6) Attend Card Access Vendor Meetings

7) Maintain close liaison with the Crime prevention officer on Card Access problems and improvements.

8) Develop and maintain written instructions, procedures, policies, and training outlines

9) Respond to after hour emergencies.

POLICY AND PROCEDURE # 82
b. Electronic Security

1) Conduct physical security surveys to improve the security of campus facilities by identifying security weaknesses and recommending corrective actions. Where the results of these surveys indicate a need for greater security, identification of personnel using the facility or the loss of a key would create a serious problem, investigate card access as a viable solution.

2) When a facility is designated as a candidate for card access, conduct a detailed inspection to identify the necessary equipment. Once this equipment is identified, obtain a quotation from the card access contractor.

3) Provide written recommendations on installing card access systems to University and College Officials. To allow these officials to make knowledgeable decisions, the Electronic Security Specialist must be prepared to explain the operation of the system in detail and promote its cost-saving advantages.

4) During the installation of a card access system, monitor all work to ensure proper installation and assure all contractual requirements are met.

5) Provide technical support to the System Administrator on card access equipment installation and operation to support system operation and monitoring of the system.

6) Be the sole point of contact with card access equipment/installation companies for all equipment malfunctions or repairs.

7) Conduct periodic quality assurance checks to ensure operability and material condition of all card access equipment, i.e., review system history to identify card access readers that are failing.

c. Administrative Support personnel

1) Ensure all requests for Card Access are approved by authorized personnel.

2) Responsible for setting up and maintaining Card Access system computer files.

3) Liaison with the official in charge of the card access facility or
his/her designee to determine requirements and to obtain required approval signatures.

4) Ensure Dispatchers have current access lists from the Card Access computer.

5) Maintain necessary files and records of all issued cards and applicable receipts.

6) Approve all Card Access requests.

7) Program / re-program door opening schedule to meet the needs of the clients.

d. Dispatcher personnel

1) Deactivating Access cards.

2) Manually Opening Doors.

3) Manually Opening Doors for extended periods.

4) Manually Closing Doors.

5) Acknowledge & Resolution of Alarms.

6) Record activities in CAD Systems.

3. Training

a. The Program Manager will train the Administrative Support personnel on the Technical aspects of Card Access System.

b. System Administrator will be a responsible for training as indicated.

1) Administrative personnel

   a) The procedure to setup and issue Card Access accounts.

   b) The procedures to deactivate a Card Access account.

2) Dispatch personnel

   a) The procedures to deactivate a Card Access account.

POLICY AND PROCEDURE # 82
1. What to do if proper forms are not obtained after hours.

2. Input information into the computer program

3. What complaint type to input into the CAD system.

b) The procedure for manually opening & closing doors.

1. Procedure for Manually Opening Doors.

2. Procedure for Manually Opening Doors for extended periods.


4. What complaint type to input into the CAD system.

c) The procedure for Acknowledgement & Resolution of Alarms

1. Procedure for Acknowledgement & Resolution of Alarms.

2. What complaint type to input into the CAD system.

4. Equipment

a. Computer, Printer and Software.

The software and the computer it is loaded on, document and maintain all actual or attempted entrances to the buildings or rooms controlled the Card Access program. Alarms are recorded on the computer and are output to the printer for a hard copy record.

b. Card Readers

An input device that allow the system to read the encoded card information to determine if the card holder has access to the area being controlled by the system.

c. Motion detectors & contact alarms on doors.

Input devices that provide the system with information on what is happening with a specific door or other entrance being monitored by the
system.

5. **Maintenance**

   a. The System Administrator is responsible for the Card Access Computer.

      1) Be the sole contact with CCIT for repairs to card access computer equipment.

      2) Conduct periodic quality assurance checks on the card access computer system.

         a) Software

            1. Test communication between computer and building.

            2. Check for allocation errors using scandisk program.

         b) Hardware

            1. Run Scandisk & Defrag programs to test the computer’s hard drive.

            2. Run bench mark tests for speed etc., using Check it software.

            3. Clean computer interior and printer of dust.

   b. The Electronic Security Specialist is responsible for all remote hardware repairs.

      1) Be the sole contact with card access companies for repairs to card access equipment.

      2) Conduct periodic quality assurance checks on card access equipment.

   c. Administrative Support is responsible for setting up and maintaining Card Access system files.

6. **Activating Cards**

   a. Requests for card access are approved and processed after receiving either
an e-mail or a phone call by the designated department manager.

b. Cards will be activated at MUSC Public Safety Headquarters Monday - Friday from 7:30 A.M. to 4:30 P.M.

7. Deactivating Cards

a. Loss of a card or termination of a cardholder must be reported to MUSC Public Safety at 792-4196 as soon as possible. Personnel are on duty 24 hours a day seven days a week for the deactivation of card keys.

b. The following procedures will be followed when this department is informed that a person has lost or has had their card access key stolen. During normal business hours the Admin. Staff or the System Administrator will handle deactivation. At all other times these duties will be handled by the Dispatcher.

1) Verify the card holder identity with proper ID.

2) From the access list obtain the Code Number of the lost card

3) Carry out the procedure on deactivating Card Access cards.

4) Lost/stolen cards will be replaced upon application using a New Issue/Replacement form and payment of a fee of $15.00. New cards will be issued during normal business hours, at Public Safety Headquarters Monday - Friday from 7:30 A.M. to 4:30 P.M.

5) All after hour deactivations must be reported to the System Administrator, with a PSD-11, so the proper action can be taken.

c. The following procedures will be followed when this department is informed of a card holder who is terminated.

1) The Supervisor of the terminated employee will contact Public Safety by e-mail or phone. A note of the change will be entered into the comment section of Entra Pass.

2) After hour requests can be verbal with the understanding that the proper paperwork will be filled out on the next business day.

3) From the access list obtain the Code Number of the lost card

4) All after hour deactivations must be reported to the System Administrator.
8. Manually Opening & Closing Doors

a. Manually opening doors on the Card Access computer. Upon receiving a complaint that a card will not open a door the dispatcher will accomplish the following.

1) Check the Active Code list to see if the person’s name is on the list.
   a) MUSC List
   b) VA List

2) Check Entra Pass

3) If the person desiring access is authorized in the requested area, dispatch an officer to verify the person’s identification using the criteria below and log the call in the CAD system. The complaint type will be CARDKEY.

4) Officer will except as forms of Identification the following.
   a) Driver’s License;
   b) MUSC or VA ID card;
   c) Passport;
   d) State ID card, Military ID card, etc....; or
   e) A signature base form of identification such as a Social Security card, Voter Registration, etc...

5) Upon verification the Dispatcher will follow the instructions for on manually opening doors. Manually Opening Doors & 2d, Manually Opening Doors for Extended Periods.

b. If an employee has forgotten their card and request access, follow the procedure in paragraph 8a3), above.

c. Manually closing doors on the Card Access computer. Upon receiving a instructions to manually close a door the dispatcher will accomplish the following.
1) The dispatcher will follow the instruction for manually closing a door in the Card Access computer.

2) Log the request in the CAD system. The complaint type will be **CARDKEY**.

9. **Acknowledge & Resolution of Alarms**

   If a door is forced open or is held open too long, an alarm will be initiated in the form of a continuous beep. It will continue until the alarm is acknowledged on the computer. The alarm will be flagged in red and blinking the word *ALER T*. The Time/Alarm/Door information will appear on the screen. If this happens accomplish the following:

   a. Follow the instructions provided on the screen and the written procedures.

   b. If you receive a restore within one minute acknowledge & resolve the alarm. In this case don’t dispatch an officer to the scene. No comments are needed in this case.

   c. If you don’t receive a restore within the given time period, dispatch an officer to the scene. When the situation is resolved type a comment in the field provided on the screen. Also record the Alarm in CAD as compliant type “**ALARM C**”.

   d. Return to the Alarm Monitoring Screen.

10. **Procedure for Fire alarms in Card Access buildings**

   a. **AT PRESENT** (Thurmond Gazes Building), In case of a fire alarm in a card access controlled building the following actions, in addition to normal code red procedures, will be taken by the dispatcher:

   1) During periods when the building is normally open. Determine if there is an actual fire and not a system malfunction. In case of an actual fire, unlock the doors on the 7th and 8th floors using the procedure in attachment 2d Manually Opening Doors for Extended Periods.

   2) Outside of normal working hours. Determine if there is an actual fire and not a system malfunction. In case of an actual fire, unlock all card access doors using the procedure in attachment 2d, Manually Opening Doors for Extended Periods.
b. **AFTER SYSTEM MODIFICATION.** In case of a fire alarm in a card access controlled building, all card access controlled door will automatically unlock. Dispatched personnel should carry out normal code red instructions.

11. **After Hours Operations**
   
a. All after hour operations will be conducted in the dispatch office.

b. No Access card will be added to the system during this time.

c. Dispatchers will monitor the system for alarms and take action when necessary.

d. Dispatchers will open and close doors as authorized by this procedure.

e. When Access cards are reported lost or stolen after hours the dispatcher has the authority to deactivate the cards. Also, the same capability applies if a card holder is terminated after hours.

f. All actions will be recorded in the CAD system.

12. **Procedure in case of a system malfunction**
   
a. All system malfunctions will be reported at once to the System Administrator or the designated back up personnel, 24 hours a day seven days a week.

   1) Designated backup personnel for the System Administrator.

   a) Administrative Support personnel.

b. The System Administrator will determine how to best resolve the problem.