THE POLICIES AND PROCEDURES INCLUDED IN THIS MANUAL ARE NOT A CONTRACT OF EMPLOYMENT AND SHOULD NOT BE RELIED ON AS SUCH. THESE POLICIES AND PROCEDURES ARE SUBJECT TO AND MAY BE CHANGED AT ANY TIME BY THE DEPARTMENT OF PUBLIC SAFETY, MEDICAL UNIVERSITY OF SOUTH CAROLINA.

A. Purpose

To establish general guidelines and procedures for the operation of the communications function.

B. Policy

The communications section plays a vital role in the Public Safety Department. It is the policy of this Department to operate an effective and efficient communications center. The Department will comply with all applicable rules and regulations of federal, state, and local governments.

C. Administration

1. The communication function is a component of the Operations Support Commander’s (OC) Office. The OC is responsible and accountable for all operations of the communications function.

   a. Chain of Command

      The Chain of Command for the Communication Section will be as follows:

      1) Chief;
      2) Operations Support Commander;
      3) Asst. Operations Support Commander;
4) Communications Supervisor; and

5) The Dispatchers on duty will be responsible to the Public Safety Supervisor on duty. In the event of a problem the Public Safety Supervisor will take whatever action he/she deems necessary and make a written report to the communications supervisor the next working day.

b. The Operations Support Commander (OSC)

1) The OSC will have the ultimate responsibility for the communications center on a twenty-four hour, seven day operation.

c. The Communications Supervisor

The Communications Supervisor shall coordinate with the Operations Support Commander on the overall operation of the communications center. The responsibilities of the Communications Supervisor will include, but not be limited to, the following:

1) The Communications Supervisor will ensure that a Training Manual for communications personnel is utilized for initial training of new communicators. He/she will ensure that the information is accurate, properly documented, and constantly reviewed for any required updates.

2) The Communications Supervisor will monitor the use of overtime and properly prepare payroll documentation for all personnel assigned to the communications function.

3) The Communications Supervisor shall approve the use of annual leave by communications personnel.

4) The Communications Supervisor will ensure that all established procedures are followed, and recommend changes to overall communications policy as required.

5) Assist in the day-to-day operation of the communications center and supervision of communications personnel. The Supervisor will ensure that the unit is properly staffed at all times for the proper performance of require duties.
6) Ensure that the Desk Reference Manual is current and accurate. The Communications Supervisor should ensure that the book is properly indexed and that information is *immediately accessible* to communications personnel. He/she will periodically contact University Departments and agencies to acquire any information changes.

7) Administer training and maintain copies of training files for all telecommunications officers.

8) Ensure that all communications equipment is maintained in appropriate working order, consult maintenance personnel as appropriate, and provide for substitution of equipment when necessary;

d. All radio operations conducted by the Department of Public Safety will be in accordance with Federal Communications Commission (FCC) guidelines and regulations. Station identification will be made every thirty minutes. Employees will not transmit any messages that would violate FCC regulations. 

(CALEA 81.1.2)

D Communication Center

1. Access to the Communications Center will be limited to authorized personnel only. It is important that communications personnel are allowed to operate in an atmosphere that is free of unnecessary noise and distractions. Access to the Communication Center will be granted by the communication personnel only after visual identification, using the CCTV system.

2. Authorized employees requiring non-emergency information from the NCIC computer will submit a request to the Communications Supervisor. The Communications Supervisor will notify the requesting party when the information has been retrieved.

3. It is necessary to keep all keys, equipment, and communications disks secure. It is therefore necessary to keep the Communication Center locked at all times.

4. The Communications Center is often the only point of contact with the public. It is the responsibility of communications personnel to ensure that the communications center is kept clean and free of trash. A professional image must be maintained at all times.

5. The communication personnel will have immediate access to the below listed
items. These items will be located in the Communication Center:

a. Personnel duty roster; (CALEA 81.2.5.b)

b. Telephone numbers of all departmental personnel; (CALEA 81.2.5.c)

c. Visual maps detailing the department’s service area (CALEA 81.2.5.d)

d. Officer status indicator; (CALEA 81.2.5.e)

e. Emergency Check List with all the emergency and external contact telephone numbers; (CALEA 81.2.5.f)

f. Tactical/operational dispatch plans; (CALEA 41.2.1, 81.2.5.g, 81.2.6.a).

1) Response to some situations or incidents will require the presence of two or more officers to effectively and safely deal with the problem. Situations requiring the response of at least two officers include, but are not limited to: (CALEA 81.2.4.e.,g)

a) Potential or actual assault on an officer;

b) Possibility of or an actual on-scene arrest for a felony or violent misdemeanor;

c) Potential or actual resistance to arrest;

d) Possibility of or actual use of force;

e) Crime in progress;

f) Fleeing suspect;

g) Presence of a suspicious person under dangerous circumstances; and

h) patient restraint request.

2) Dispatchers and supervisors will insure that at least two (2) officers are dispatched in response to the above incidents. Officers who observe such situations will immediately notify the Dispatcher and request back-up. Responding officers should coordinate their simultaneous arrival, if possible.
The emergency check list establishes the requirements for Supervisors to be at the incident location and or special occurrences; (CALEA 81.2.f)

1) The Shift Supervisor must be notified of and respond to all serious, unusual, or questionable situations. The following are examples of situations requiring the presence of the Supervisor: (CALEA 81.2.6.a)

a) Injury to an officer;

b) Accident involving a police vehicle;

c) Major crime;

d) Complaint against an officer;

e) Accidents, injury, or incidents involving employees, students, patients, visitors, or property;

f) Incidents involving the use of force;

g) Loss or theft of Public Safety property;

h) Requests for assistance of any kind from a school president, department head or VIP;

i) Discovery of a serious safety hazard; and

ej) Patient restraint.

Communication will have 24 hour access to the on duty public safety Supervisor and are authorized to call any member in their Chain of Command when the need arises. (CALEA 81.2.5.a)

When there is one dispatcher on duty, the dispatcher is to request the meal break (30 minutes) through the supervisor that is on duty. The supervisor will assign a Public Safety Officer to relieve the dispatcher. The dispatcher will remain in the Public Safety Building during the break. The only time the dispatcher will be paid for a meal break is when the shift supervisor is unable to provide a relief officer. The dispatcher will write an Intra-Departmental Correspondence (PSD-11) explaining the circumstances and a signed Kronos Time Entry Form for the Communication Supervisor.
E Communications Equipment

1. The Communications Center operates four radio channels. Telephone and radio transmissions are recorded on a twenty-four hour basis.

2. All recordings are kept on the digital audio recorder for ninety (90) days (CALEA 81.2.8.a). The digital recorder is backed up by the TSM software to the University SAN system. The system is located in the main computer room located at 100 Doughty Street. This area is controlled by card access and video surveillance. (CALEA 81.2.8.b)

3. The communications equipment has the capability of immediate playback of recorded telephone and radio conversations while it maintains a continuous recording of radio transmissions and emergency telephone conversations. All communications personnel will be trained to perform this procedure to retrieve emergency information. Except under emergency circumstances, employees will not review recorded conversations without the permission of the Chief, Patrol Commander, Operations Support Commander. (CALEA 81.2.8.c)

4. Request for CD copies from sources outside the Department will require a subpoena or the express prior approval of the Chief, or his designee. In the event of a subpoena, the party requesting may be responsible for reimbursement of any expense involved in making such a copy.

F. General Operations

1. The communication function is responsible for twenty-four hour, seven day operation of the Communications Center, to include, but not be limited to, the following:
   a. Telephone communications;
   b. Teletype and automated data communications;
   c. Radio communications;
   d. Alarm monitoring systems;
   e. Pawn pager;
   f. Assistance to visitors to the Medical University of South Carolina;
   g. Card Access; and
h. CCTV

i. Call Boxes

j. TDD System (telecommunication device for the deaf)

2. The authority of the Dispatcher may only be countermanded by the Shift Supervisor or a senior law enforcement officer of the rank of Lieutenant or higher.

3. The taking and recording of complaint reports and offense reports from individuals with telephonic information concerning an incident that occurred within this agency’s jurisdiction should be handled with continuity and uniformity by all personnel. (CALEA 82.2.5)

   a. Officers, when assigned to handle telephonic complaints will ascertain the following information. Determine the type of incident that exists, determine if a report is necessary for the Department to address.

      1) Is the incident in progress?
      2) Is the perpetrator known?
      3) Is there a crime scene that needs a police officer or investigators attention?
      4) Are there witnesses available?
      5) Can the location of the offense be established?
      6) Cases of Property;
         (a) Is this a case of theft, lost or missing item?
         (b) Is documentation provided as to ownership and value?

   b. When it has been determined that the Department will address and record the incident, the information will be placed on an incident report.

      1) The officer receiving the complaint will advise their supervisor of unusual facts and information received. The assigned officer should weigh the facts and if required, a sworn statement will accompany the complaint.
      2) The supervisor will review all paperwork for completeness
and accuracy prior to its submission to the Records Specialist.

4. The communications Dispatcher will have responsibilities that include, but are not limited to, the following:

a. A daily assignment sheet will be maintained continuously, either written or automated. Entries will include, but not be limited to:

1) A beginning of shift log indicating the status of each person on the shift,

2) The unit number of each officer on-duty;

3) Any equipment breakdowns or malfunctions, who, if anyone, was notified;

4) Any equipment missing / removed from the Communication Center

b. The CAD Log will be used by communications personnel to record status of officers, assignment of officers to calls and all requests for service, to include those received by telephone, in-person, self-initiated by officers, or reported by officers in the field. Supervisors and officers will be assigned to calls in accordance to Patrol Procedure #68. Officers are required to communicate with dispatch in accordance to Patrol Procedure #68 (CALEA 81.2.4.a). The CAD Log will indicate the status of every officer on patrol and will include the following:

1) OCA or CAD number; (CALEA 81.2.3.a)

2) Date and time of request; (CALEA 81.2.3.b)

3) Name and address of complainant; (CALEA 81.2.3.c)

4) Type of incident; (CALEA 81.2.3.d)

5) Location of incident reported; (CALEA 81.2.3.e)

6) Call sign of all on duty officers; (CALEA 81.2.3.f and 81.2.4.c)

7) Officer status, in service or out of service; (CALEA 81.2.4.b, 81.2.5.e)
8) Officer assignments;
9) Location of officer(s) assigned as primary and backup;
10) Time of dispatch; (CALEA 81.2.3.g)
11) Time of officer arrival; (CALEA 81.2.3.h)
12) Time of officer return to service; (CALEA 81.2.3.i)
13) Disposition or status of reported incident; and (CALEA 81.2.3.j)
14) Call back telephone number.

c. A loose leaf book will be maintained at the communications desk as a "Daily Read File" for all communications personnel. This book will be used to “pass along” information of relevance to other communications personnel. Communications personnel will check this book at the beginning of each tour of duty.

d. The Dispatcher will promptly redirect all mis-directed phone calls. If the call is an emergency the dispatcher will take the call and relay the information to the appropriate agency. (CALEA 81.2.12)

e. The campus has been organized into patrol zones. The purpose of the zones is to reduce the volume of radio traffic by calling in zones rather than each facility. As officers patrol their post, they must 10-23 and 10-24 each zone. Officers are required to call in under the following circumstances: (CALEA 81.2.4.a)

1) Officer entering a building;
2) There is an emergency;
3) Something needs to be investigated;
4) Some kind of police or security action is required;
5) Each officer will communicate with Headquarters at least once an hour; or
6) If in doubt, call in.
G. Telephone Communications

1. Answer promptly. Try to answer on the first three rings. Even if there are several calls to answer at one time, at least answer and put the person on hold, if appropriate. Find out first what the purpose of the person's call is, to determine if they can be put on hold.
   a. The Communication Center will have a single 24 hour toll free emergency telephone number. (CALEA 81.2.1) This number will be a seven line number to prevent a caller from getting a busy signal when calling. All calls of a non emergency nature will be immediately transferred to the non emergency number.
   b. The Communications Center will have a non emergency number. This number will be a 2 line number. (CALEA 81.3.3)

2. Announce Your Identity. Let the person on the telephone know what agency and operator they have contacted, and that assistance is available to them. (Example: Public Safety, Operator two, how may I help you?)
   a. If answering the emergency line, answer in the following manner: "Emergency line, Public Safety, please state your emergency.”
   b. If answering the emergency line and no one responds to inquires, attempt to make contact with a possible complainant by calling the number back. In the event no one is reached, dispatch a unit.
   c. Non-emergency calls to the emergency line should be transferred to the non-emergency number. Communications personnel should advise the caller that the emergency line is dedicated to emergency requests ONLY.

3. Speak directly into the mouthpiece. The operator will be properly understood and not waste time in having to repeat information.

4. Be calm and courteous. Use a calm, decisive, professional sounding voice.

5. Call the caller by his or her name. This helps to reassure them because they are recognized as a person.

6. Take control of the conversation. When you sense what the caller's problem is (for example he says "Help, I've been robbed," or "I have just seen an accident take place") cut off unnecessary verbiage by asking questions. This will keep the caller from delaying time by giving you unneeded information.

POLICY AND PROCEDURE # 64
7. Obtain as much information as possible. Never leave anything to memory. An informed police officer, who is assigned a call, will be able to act more efficiently and safely.

8. Delays are irritating to the caller. Remember, this call is the most important call we receive in the mind of the caller. If it becomes necessary for a caller to wait, tell him/her why, and that you will return to him/her as soon as possible.

9. Show some interest in a person's call. The caller needs assistance or information that he/she feels is important to him/her.

10. Never give a caller information that has not been verified. Instead, refer them to the proper person or agency or, time permitting, you may contact the proper person and return the information to the caller.

11. Transfer calls only when necessary, advise the caller what you intend to do and to whom he/she is being transferred.

12. The telephone should be used for official business only. Personal calls should only be made after the tour of duty or during breaks.

13. Always end the telephone conversation with a positive note. For example: "Thank you for calling, Mr. Jones. We will have an officer take care of this as soon as possible." Never give a caller a definite length of time. Simply leave the conversation with "as soon as possible."

14. The following information is needed on all calls:
   a. **WHO**: Who is it who is calling and what is their call back number and location?
   b. **WHAT**: What is the call about?
   c. **WHEN**: When did the incident take place: today, five minutes ago, yesterday?
   d. **WHERE**: Where is this incident occurring? Where is the officer to go?
   e. **WEAPONS**: Are there any weapons involved? If so, what kind? (Guns, knives, bottles, etc.)

15. In cases where the caller insists on remaining anonymous, do not persist, but obtain the other required information.

**POLICY AND PROCEDURE # 64**
16. Avoid law enforcement jargon, slang or codes while talking on the telephone. The general public does not understand these terms.

17. During the course of any day, the Communications Center may receive calls from victims or witnesses requesting information or services. In talking with the victims or witnesses, communications personnel must obtain necessary information to judge the characteristics of the call to determine whether an emergency or non-emergency response is required. (CALEA 81.2.6.a) In most cases the Department’s Victim Advocate be notified.

18. Communications personnel will inform the victim or witness of the Department’s response, either direct law enforcement, referral to the Victim Advocate, or referral to another agency. (CALEA 81.2.6.b, 81.2.7)

19. All communication personnel should familiarize themselves with the service area of the Department of Public Safety. Emergency calls that are not within the Department’s service area should be routed to the proper agency in accordance with the following guidelines.
   
a. Communications personnel receiving non-emergency calls on an administrative line should give the caller the phone number of the appropriate agency he/she should contact. This information is obtainable utilizing the desk reference book.
   
b. Communications personnel receiving an emergency call on an administrative line should obtain the information just as though we were going to handle the call, and that information should then be given to the appropriate agency by the dispatcher handling the call.
   
c. On the emergency lines, the caller should be told that the call is being transferred, and the dispatcher should then effect the transfer, staying on the line to ensure the connection is good and the appropriate agency receives the information. (CALEA 81.2.6.b)

20. The Dispatcher will take all messages for Department employees in their absence and are responsible for forwarding these messages to the employee. Employees who receive telephone calls requiring immediate attention WILL BE NOTIFIED IMMEDIATELY.

21. Acceptance of citizen calls regarding the delivery of emergency messages will require that the dispatcher be able to validate the nature of the emergency through a law enforcement agency, hospital, coroner or other competent source. Once validated, a call for service will be entered and dispatched for delivery by the next

POLICY AND PROCEDURE # 64
available unit in that area. (CAEA 81.2.11)

22. The function of communications personnel is not to determine whether a particular location is in or out of the Department’s service area, or if a police officer should be sent on a particular call. If a call is received where there is a question, the Public Safety Supervisor on duty will make the determination, NOT the Dispatcher. If another agency is refusing to respond to a call believed to be outside of our service area, the on-duty supervisor will be notified and make whatever determination he/she believes to be proper.

23. Always speak and act PROFESSIONALLY

24. This agency is prohibited from giving first aid instructions over the phone. (CAEA 81.2.14)

H. Teletype Communications

1. All communications personnel will attend and successfully complete the NCIC/SLED Certification training within six (6) months of assignment in the Communications Center.

2. No un-certified personnel, other than communications personnel in training, will be allowed to operate the SLED/NCIC terminal (CAEA 82.1.7).

3. All utilization of the SLED/NCIC terminals shall comply with the rules and regulations outlined in the NCIC Operator's Manual located in the Communications Center.

4. The FBI/NCIC requires that each department or agency possessing a computer terminal that accesses the NCIC files appoint an individual to serve as liaison and TAC for all related FBI/NCIC matters. This individual should be a supervising/management position with a degree of authority which will ensure that all FBI/NCIC policies, procedures, rules and regulations are adhered to. The Department should appoint an Alternate TAC to serve when the TAC is unavailable. Both the TAC and Alternate TAC will be NCIC certified based on the level of functionality that is assigned to the terminal located in the agency.

   a. The Chief will appoint the Terminal Agency Coordinator (TAC) and has the sole authority to name or change the Terminal Agency Coordinator at his/her discretion. The Chief may change the TAC by submitting a new form. The TAC should immediately be changed when the current TAC is reassigned or leaves employment with the Department.

5. Duties of the Terminal Agency Coordinator (TAC) include but not limited to:

POLICY AND PROCEDURE # 64

13
a. Receipt of all FBI/NCIC, SLED and CJICS information concerning the communications network, state and national files. Ensures distribution of material within department to appropriate personnel.

b. Attend scheduled TAC meetings and seminars.

c. Coordinates the scheduling of individuals for certification.

d. Ensures compliance with all FBI/NCIC policies, procedures, etc.

e. Responsible for the security of all terminal equipment accessing the FBI/NCIC system.


g. Coordinate any relocations, etc., of the computer terminal equipment with SLED.

h. Function as liaison as deemed necessary and appropriate during mandated audit of Departments use of the FBI/NCIC system.

i. Maintain all training records for terminal operators.

j. Responsible for implementing the designated reaffirmation procedure for each certified terminal operator as directed by SLED/CJIS NCIC training.

k. FBI, CJIS Security Policy: the required deleting of passwords, log-on, etc. of separated employees by advising SLED within 5 days upon learning of separation.

I. Alarm Activations / MUSC

The Dispatcher upon receiving an alarm activation will immediately check the alarm receiver/computer for the account number codes which have activated. Upon checking the receiver/computer for the activated alarm. The Dispatcher will immediately determine the type of alarm by the account number indicated to ensure that proper units are dispatched and/or personnel notified.

1. The Dispatcher upon receiving an audible alarm from the receiver/computer should check and verify the account number generated by the alarm activation. Click TELEPHONE ICON – account information will be displayed on the screen.
2. Upon interpreting the information in the alarm manual, the Dispatcher shall immediately dispatch a primary and secondary unit to the scene. The Dispatcher will transmit detailed information to the officer(s) responding, indicating the type of alarm, building name, room number, and street address and/or other pertinent information about the alarm.

3. The Dispatcher shall then attempt to contact person(s) listed on the emergency notification list during normal working hours. After normal working hours, the emergency notification list should only be utilized in the case of an emergency such as burglary, fire, broken glass, damage to office/personal equipment, medical emergencies, injuries, suspicious activity, etc. This procedure should be followed unless otherwise directed by the instructions displayed on the computer for the account in question or for any other associated problem which may warrant notification.

4. Upon establishing contact with personnel at the alarm location, the dispatcher shall advise the responding officer(s) of any pertinent information or status regarding the alarm, as well as the location of the personnel, in order to ascertain the nature of the problem and to ensure proper assistance is rendered.

5. The Dispatcher shall record any information pertaining to the alarm activation on the radio/CAD log and shall enter the information into the receiver/computer indicating the following information: causes of the alarm activation, the names of personnel at the scene, and if the alarm was attributed to employee/staff error.

6. For notifications of the fire department, physical plant and public safety personnel follow these procedures:

   a. MUSC / CMH Fire Alarms

      If the initial alarm is received by department communication staff, the Dispatcher will call the Charleston Fire Department, Physical Plant and dispatch two public safety officers. If the initial alarm is received by CENTREX, it is the responsibility of CENTREX to notify the Fire Department and Physical Plant, all other notifications will be made by the departmental communication staff. Responding officers will respond to a fire alarm as an “emergency call.”

7. The IT Section will evaluate, at least once every two years, the security situation that prompted the installation of the panic alarm to ensure the security need is still relevant and being met.

J. Alarm Activations / Off Campus Sites
At the moment an alarm activates from an off campus location, the Dispatcher shall notify the law enforcement agency having jurisdiction to respond to the alarm activation, unless otherwise specified by the directions displayed on the computer screen. The Dispatcher shall also immediately notify the on duty Public Safety Supervisor and the emergency contact listed on the account.

K. Alarm Malfunctions

The Dispatcher shall notify the "on call" alarm technician immediately for any emergencies relating, but not limited to, continuous false alarms, repeated activation's, vandalism of equipment, or other problems associated with inoperable burglar/fire alarm systems. The Dispatcher shall report non-emergency problems, such as low battery alarms, to the voice mail of the "on call" alarm technician, unless otherwise instructed. The Dispatcher shall immediately notify the physical plant for any building fire alarm activation, alarm trouble, or other problems associated with fire alarms and/or inoperable systems.

L. Radio Communications

All on duty personnel will carry a portable radio. Radio communications between duty personnel and communication will be controlled by the Dispatcher. Care must be taken to ensure that radio communication is available 24 hours a day. Any malfunction with the radio system will be reported immediately to the communication supervisor. (CALEA 81.2.2)

1. The Dispatcher position is one of control, expected to promote an orderly and legal operating procedure.

2. All communications personnel must remain calm and in complete control at all times. One who becomes confused, unsure, or excited during emergencies is of no value to the Department and can be detrimental to the safety of officers and/or the public.

3. The safety of the officers and the public depends upon the alertness and efficiency of the Dispatcher. Personnel in the communications center will allow nothing to distract their attention from their duties.

4. The Dispatcher will immediately act upon any orders received from the shift supervisor, or from the scene of an incident, unless advised otherwise by the Operations Support Commander, or Communications Supervisor. In the event that any order supersedes existing rules, regulations, General Orders and/or memoranda, the Dispatcher will reduce the incident to writing for his/her superior.
5. The Dispatcher must not leave the operating position at the control desk unless absolutely necessary, and then only by means of a relief who has been fully briefed on the current status of all units under his/her control.

6. In communicating with a field unit, the dispatcher will include the unit number and time upon completion of the transmission. At no time will a unit be acknowledged without using the unit number to ensure that the unit is aware of whom the communications officer is addressing. (CALEA 81.2.4.c)

7. The voice of a Dispatcher should give the distinct impression that he/she is alert and ready for any emergency. The voice should be impersonal, clear, instant and completely ready to serve. A Dispatcher will never sound bored or give the implication that he/she is doing the officer a favor by answering the radio.

8. Never acknowledge a transmission unless you are absolutely sure of its accuracy and that you understand it.

9. The Dispatcher will always consider the SAFETY OF THE OFFICER. If an officer checked off the air on a complaint and is not back in service within a reasonable period of time, attempt to call him/her on the radio. If the officer cannot be reached after two attempts, the Supervisor on duty will be contacted immediately and advised. The officer in question may be hurt or having radio trouble; it is up to the Supervisor to make that determination.

10. Use codes whenever possible. Codes replace words, they are not to be added to words.

**WRONG**

AWhat is your 10-20?"
"You've got a 10-50 at..."
"Can you 10-21 Ms Smith?"

**CORRECT**

"10-20?"
"Respond to 10-50 at"
"10-21 Ms Smith"

11. A message should be short and concise. Use the codes as much as possible.

12. Avoid phrases and words that are difficult to copy:

**POOR**

"want"
"buy"
"do you want"
"call and see"

**PREFERRED**

"desired"
"purchase"
"advise if"
"check"

13. During an emergency situation, the Dispatcher will immediately clear the air by
announcing, "All units 10-12," and continue with the information. The Dispatcher will advise all units to keep traffic on the air limited to EMERGENCY TRANSMISSIONS ONLY until the situation is under control.

14. When external services are required by officers for any situation, the Dispatcher will utilize the Dispatch Desk Reference Book. The Communications Center is responsible for interacting with other agencies, as needed. (CALEA 81.2.4 d)

**M Policy and Procedures for NCIC / CJICS Computer (CALEA 81.2.9)**

This Department has a NCIC terminal and will operate it in accordance with established FBI and SLED guidelines. In establishing such written policy directives, it is impossible to anticipate every possible situation, however, the lack of a policy or rule shall not lessen the requirement that good discretion and judgment must be exercised in the performance of your duty at all times.

1. Only authorized persons are allowed to operate the SLED CJICS/NCIC computer terminal. Authorized personnel include the dispatcher, and all individuals having successfully passed the SLED NCIC Computer class or pre-test. The Division of Law Enforcement and Safety will conduct background investigations on all SLED/CJIS-FBI/NCIC terminal operators, to include the submission of a completed applicant fingerprint card to the FBI-Identification Division through SLED. This is accomplished during the hiring process for all public safety officer positions and will be referred to when an employee is considered for transfer to a terminal operator position.

2. The Communications Supervisor, when considering an officer for reassignment to a terminal operator position, will first conduct a search of state and national criminal history files using purpose "J" and a state and national fugitive search (Wanted Person check) through SLED/CJICS-FBI/NCIC System using the officer's full name, date of birth, race, sex, and social security number.

3. If a record of any kind is found, terminal access will not be granted, at that time. The officer being considered for the assignment will be notified that the consideration has been delayed pending review of criminal history records and/or fugitive records and a final decision by the Chief.

4. The TAC will forward the considered officer's fingerprint card and written notification of any negative information disclosed in the search of criminal history/fugitive records to the State CTO. The final decision to afford or deny terminal ACCESS will be made by the State CTO after considering the public's best interest. If the dispatcher has a problem with any SLED computer operation, and has exhausted all means to correct the problem themselves, the SLED computer room should be contacted for assistance. The SLED computer is to be
used for official law enforcement business only. For all items not specifically covered in the procedure outline, refer to the NCIC Operating Manual for additional instructions.

5. The Dispatcher receives all incoming teletypes and must distribute them to the proper individual or department. The Dispatcher enters all missing persons, wanted persons, unidentified persons, weapons and license plates into the computer at the time the Incident Report or Supplemental Incident Report is made. Articles are entered into NCIC after the Investigator verifies serial numbers, model numbers and descriptions. The original Incident Report or Supplemental Incident Report should reflect NCIC entry. The Dispatcher will complete the NCIC Entry Quality Check Form and or Wanted Persons Form on any type of entry.

6. All messages sent to other agencies that require a reply will be retained by the requesting individual or by the Shift Supervisor. If a teletype is received that would be of interest to all police personnel, including BOLOs, Academy class announcements, etc., the Dispatcher should make copies for the appropriate personnel.

7. Hit Confirmation

**DEFINITION**- *NCIC Operating Manual, Introduction Section 3.5*

A **hit** is a positive response from NCIC in which the person or property inquired upon appears to match the person or property contained in the response.

**HIT CONFIRMATION PROCESS**- *NCIC Operating Manual, Introduction Section 3.5*

Agency which receives a hit on a record must:

a. Ensure the person or property inquired upon is identical to the person or property identified in the record.

b. Determine the appropriate priority level

   - **Urgent**: Confirm within 10 minutes - The hit is the only basis for detaining a suspect or the nature of the case requires urgent confirmation of a hit.
   - **Routine**: Confirm within 60 minutes - Used when the person is being held on local charges, property has been located under circumstances where immediate action is not necessary, or an urgent confirmation is not required.

c. Contact the agency that entered the record to confirm the information, if the whereabouts of the person or property is known.

d. Ensure the warrant, missing person report, protection order, or theft report is still outstanding

   - Obtain a decision regarding the extradition of a wanted person when applicable
• Obtain information regarding the return of the missing person to the appropriate authorities
• Obtain information regarding the return of stolen property to its rightful owner
• Obtain information regarding the terms, conditions, and service of a protection order

e. Following confirmation with originating agency, a locate must be entered.

Upon receipt of a hit confirmation request, the ORI of the record must:
1. Review all available information, including case file, warrants, and reports relevant to identifying the person or property to ensure that a proper response is given.
2. Furnish a substantive response within the designated timeframe
   • Positive
   • Negative
   • Notice of specific amount of time necessary to confirm or reject

MESSAGE KEYS
YQ Hit Confirmation Request
*ORI (Originating Agency Identifier) Enter the ORI of the agency sending the hit confirmation request
*DST (Destination) Enter the ORI of the agency of the record or the agency that is providing 24-hour hit confirmation for the agency of the record.
CTL (Nlets Control Field) Enter the control field number, if provided, beginning with an asterisk
*RNO (Request Number) Enter 1-first request, 2-second request, or 3-third request.
*PRI (Priority) Enter the level of priority established for responding to hit confirmation request.
R-Routine response in one hour or U-Urgent response in ten minutes
*OCA (Originating Agency Case Number) Enter the OCA found in the NCIC record
NIC (NCIC Number) Enter the NIC number of the record
*RNA (Requester’s Name) Enter the name of the individual responsible for the transmission of the message
*RAG (Agency Name) Enter the name of the agency responsible for the transmission of the message
PHO (Phone Number) Enter a contact phone number
EXT (Extension) Enter extension number, if applicable
FAX (Fax Number) Enter fax number, if applicable
REM (Remarks) Enter additional information that may aid in the recovery of stolen property, apprehension of wanted person, or location of missing person.
YR Hit Confirmation Response
*ORI (Originating Agency Identifier) Enter the ORI of the agency sending the hit confirmation response
*DST (Destination) Enter the ORI of the agency requesting hit confirmation

POLICY AND PROCEDURE # 64
CTL (Nlets Control Field) Enter the control field number, if provided, beginning with an asterisk.

*CON (Confirmation Status) Enter Y-Yes, hit is confirmed; N-No, hit is not confirmed; E-Hit is Confirmed-awaiting extradition decision; or P-In process of being confirmed

HRS (Confirmation Hours) Enter the number of hours required to confirm the status, if confirmation status is E or P.

*OCA (Originating Agency Case Number) Enter the OCA found in the NCIC record

NIC (NCIC Number) Enter the NIC number of the record

*CNA (Confirming Name) Enter the name of the individual responsible for confirming the hit

*CAG (Agency Name) Enter the name of the agency responsible for confirming the hit

PHO (Phone Number) Enter a contact phone number

EXT (Extension) Enter extension number, if applicable

FAX (Fax Number) Enter fax number, if applicable

REM (Remarks) Enter additional information that may aid in the recovery of stolen property, apprehension of wanted person, or location of missing person

*Indicates mandatory fields

When a hit 10 minute/urgent and routine hits is received it will handled in accordance with the NCIC Policy and Procedure Manual. The Dispatcher is then to search for the information in the NCIC Hot File (red binder), located in the Communications Center of the Department of Public Safety. If, for any reason, the Dispatcher cannot confirm the request (positive or negative) using the Hot File (red binder), a teletype must be sent to the requesting agency informing them of when the request may be confirmed. If the Dispatcher is unable to confirm, and it is an emergency, the on duty Supervisor will provide a copy of the original incident report.

8. Disciplinary Actions

a. Terminal operators are expected to perform their work efficiently and effectively, to be mindful of the public's expectations of the department and its employees, and to be knowledgeable of this policy’s requirements.

b. Violators of NCIC, SLED, or University Policy, are subject to disciplinary actions in accordance with the University's Policies and Procedures Manual. The purpose of any discipline is to provide constructive, instructional measures for the correction of deficiencies without having to resort to the employee's dismissal. Employees will be given the opportunity to improve their deficiencies before dismissal through the use of progressive, consistent discipline. Unless the seriousness of the violation calls for immediate action, the University's policy on recommended progressive penalties (including oral reprimand, written reprimand, suspension, and dismissal) should be complied with. Examples of such serious deficiencies/conduct which might result in dismissal on a documented first offense could be the illegal dissemination of criminal history record information or the malicious failure to enter or
clear information from the SLED/CJICS-FBI/NCIC system as directed.

c. Terminal operator job deficiencies and/or offenses which could result in disciplinary action may include, but are not limited to, categories of conduct the University's policy refers to as: careless, negligent or improper use of University equipment or property; unauthorized use of University equipment or property; destruction or willful misuse of University property or equipment; leaving work station without authorization; falsification of records; unauthorized release of records information; gross negligence; and gross misconduct.

d. All other specific guidelines for implementing disciplinary ACTION will be in ACCORDANCE with the University's HRM policy, 45

9. Wanted, Missing, and Unidentified Persons (CALEA 41.2.5.c)

a. The Reporting Officer (R/O) will have in his possession an original incident report or valid arrest warrant containing the person to be entered. The dispatcher should verify the missing, wanted, or unidentified person meets the NCIC Operating Manual criteria. (Missing Persons, Wanted Persons, {NOTE Extradition Requirements}, Unidentified Persons).

b. The officer handling the call will complete one of the following forms prior to entering the information into NCIC; Wanted Person Form, Wanted Person Form stamped Juvenile, SLED Missing Person Information Center Report form, or an Unidentified Person Form.

c. The Dispatcher will review the form for accuracy.

d. When a warrant is issued by a Charleston County Magistrate, it will be forwarded to the Investigations Section of the Department of Public Safety. If the defendant is in the Charleston County area, they will serve the warrant. If the defendant can be located in another South Carolina County, the Investigation Section may either: 1) have the warrant counter-signed and served with local authority assistance; or, 2) forward the warrant to the other county for service. If the crime is more serious or the defendant is to be extradited, the Communications Section will enter the warrant into the NCIC system.

e. The Dispatcher will then enter the information into NCIC. The Communication Supervisor will review for ACCURACY. The NCIC printout and the applicable forms will be forwarded to the Records Section.
f. The Records Section will compare all the information on the printout with the Incident Report, warrant, and the form(s) for completeness.

g. Persons - In addition to the required information listed on the Wanted Person (adult or juvenile) form, the following information is desired:

1) Place of birth;
2) Date of emancipation (juvenile);
3) Skin tone;
4) Scars, marks, and tattoos;
5) Fingerprint classification;
6) Miscellaneous numbers;
7) Miscellaneous information; and
8) Alias, vehicle/drivers license data, any stolen or fraudulent identifications.

h. To cancel or clear the Wanted Persons entry, the following information is required:

1) An Original Supplemental Incident Report showing the subject is in custody, or showing the extradition requirements have changed; the NCIC assigned number.

2) The printout showing cancellation or clear should be given to the Records Section attached to the original Supplemental Incident Report.

3) Missing Persons - In addition to the required fields indicated on the example entry attached, the SLED Missing Persons Information Center Report Form must be signed by the complainant. Documentation is required for NCIC entry and is outlined in Missing Persons section of the NCIC Operating Manual. (CALEA 41.2.5.c)

i. To cancel or clear the Missing Person entry, the following information is required: (CALEA 41.2.5.c)
1) The original Supplemental Incident Report showing the victim has been located;

2) OCA or NIC number;

3) Date of location of victim.

4) The printout showing cancellation should be turned into the Records Section along with the original Supplemental Incident Report.

j. Unidentified Persons Required fields are listed on the Unidentified Persons Form. See NCIC Operating Manual for criteria and further information on entering unidentified persons.

k. To cancel or clear the Unidentified Persons entry, the following information is required:

   1) The original supplemental Incident report showing the victim has been identified; and

   2) NCIC assigned number.

10. Stolen vehicles, license Plates, Weapons, Boats, Securities, and Articles

   a. In the SLED CTICS/NCIC Operating Manual there is a listing of required fields, message key codes and all other pertinent information needed when sending entering, modifying, canceling, inquiring, clearing, or locating messages. Refer to this section for guidelines in addition to the separate sections on each item (vehicles, license plates, weapons, boats, securities, and articles). All entries must meet the NCIC criteria.

   b. A second individual should review the printout to verify the ACCURACY of serial numbers, vehicle identification numbers, etc.

   c. The printout for all messages concerning stolen property should be attached to the original Incident Report or original Supplemental Incident Reports and turned into the Records Section.

   d. The officer will indicate on the Incident Report and/or Supplemental Incident Report the ACTION taken on the NCIC computer.

   e. If an item is entered after Records has received their copy of the Incident Report or Supplemental Incident Report, a copy of the printout should be
When canceling or clearing an article, the printout should be attached to the Supplemental Incident Report and the original sent to Records.

11. Utilizing Criminal History Files

a. Criminal history information may be requested by uniformed officers, investigators, and administrative personnel of the Department of Public Safety concerning arrests and investigations. Criminal history checks for private individuals are not authorized. If an individual or agency is interested in a complete criminal history (records from all agencies submitting fingerprint cards) they should be directed to SLED. To receive a MUSC-PSD arrest record, private individuals must complete a Request for Record Form (maintained in the MUSC-PSD Records Office).

b. When entering a request for background information on an individual using a CCH transaction (ICHS, ICHR, IQ, FQ, and AQ), the Officer will justify the request to the Dispatcher. Once a CCH request has been made, the dispatcher shall record the information requested in the ICHS/ICHR Dissemination Log. The Dissemination Log will be maintained for at least 12 months.

c. When communications personnel inquire into NCIC on criminal history records, each 'hit' should be entered in the Criminal History Dissemination Log indicating distribution of 'conviction or non-conviction' data. Printouts (positive and negative requests) of criminal history information and requests should be attached to the original Incident Report (if applicable) and delivered to the Records Section. If a negative response was received, the printouts will be attached to the incident report immediately upon receipt by the Records Section.

12. Conducting Validations and Quality Control of Records

In order to insure ACCURACY and completeness of the records entered into the NCIC system, the following procedure is established:

a. Upon receipt of the validation listing from SLED, the record clerk will begin validations by contacting victims, complainants, insurance companies, or other individuals involved in the incident, to verify the status of the property or person.

b. If the records clerk is unable to obtain positive response that the property
c. Upon receipt of the validation listing from SLED, the validations must be completed within 45 days, and the Validation Completion Letter sent back to SLED.

d. The NCIC Operating Manual gives further information on the validation requirements. NCIC records must be accurate and up-to-date. Any modifications, cancellations, or clearances must be made in a timely manner. If a serious error message ($E$) is received from NCIC concerning an entry by this agency, immediate action must be taken to include but not limited to:

1) Reviewing the original Incident Report, compare listings against archive files;

2) Verifying the serial, OAN or vehicle identification numbers, do not enter vehicle License - query SCHDHT Division of Motor Vehicles to ascertain information relative to status of license plate;

3) Removal of the item if the review indicates the item/person was entered correctly by the information received from the complainant but does not comply with NCIC edits;

4) Wanted - check with court to ensure that the court has not canceled the warrant and failed to notify this agency;

5) Missing persons - check with the legal guardian/parent or other person on the missing persons report to insure that the subject has not returned.

6) Boats, guns and valuables - check with the owner/insurance company to ensure that the property was not returned; and

7) If unable to obtain a definite, positive response, cancel the record.


The Medical University of South Carolina Department of Public Safety has signed an agreement with SLED in order to have ACCESS to the CJICS/NCIC terminal. The department has agreed to follow all the rules and polices concerning the operation of this terminal and adopts all policies and procedures set forth in the SLED/NCIC Operations Manual. All employees of the division of the Department will follow all policies set forth in the SLED/NCIC Manual and the
Department’s Policies and Procedure Manual.

a. Failure to comply with the SLED/NCIC Manual or the Department’s Policies and Procedures Manual will result in written notification from SLED to take corrective measures. If such measures are not enforced, ACCESS to the NCIC/CJICS system will be denied by SLED. Any terminal operator who fails to comply with the standards set forth in the SLED/NCIC Manual or the Department’s Policies and Procedures Manual will be subject to disciplinary action as outlined in the Department Policies and Procedures Manual.

b. All terminal operators who utilize the NCIC/CJICS system located at the Public Safety Department will be certified according to the standards set forth by SLED. Probationary employees may operate the system for training purposes, and only under the supervision of a certified operator.

14. NCIC and Probable Cause

a. An NCIC 'hit' alone is not probable cause to arrest. An NCIC 'hit' furnishes an inquirer the fact that a stolen report, missing persons report, or a warrant has been filed. A 'hit' is one fact which must be added to other facts by the officer in arriving at sufficient legal grounds for probable cause to arrest. NCIC procedure demands that the agency which places the record in file be contacted by the inquiring agency to confirm that the data is ACCURATE and up-to-date.

b. When a 'positive hit' has been received, the dispatcher will immediately advise the requesting officer of the 'hit' and that the dispatcher is attempting to contact the entering agency to confirm the 'hit'. The dispatcher will at that time, send a YQ message to the entering agency. If a YR message is not received in the allotted time, a second YQ message will be sent to the entering agency as well as to SLED (our CTA) and to the CTA or the confirming agency. If a YR message is not received in the allotted time, another YQ message is sent to the entering agency, as well as to our CTA, the entering agency's CTA, and the FBI. If no message is received from the entering agency, the dispatcher will search the ORION file to obtain that agency's address and telephone number. Upon contacting the agency by telephone, request they confirm the 'hit' or respond to the YQ message over the computer system using the YR format.

c. The Dispatcher will evaluate the information received from the entering agency. If the property or person does not match the inquiry, they will advise the requesting officer to disregard the 'hit'.
d. Whenever an NCIC inquiry yields a 'hit', the dispatcher making the inquiry will note on the terminal produced printout precisely how, when, and to whom the information was given; initial and date the notation; and forward the printout to the inquiring officer for retention in the case file.

e. Under no circumstances should an arrest be made or a vehicle confiscated based solely on an NCIC 'hit'. An NCIC 'hit' is only one piece of information necessary for such ACTION.

15. System Security

The data stored in the NCIC/CJICS terminal is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. The hardware of the system must be stored in a place inaccessible to the general public. The information within the terminal must be considered confidential and treated with the utmost discretion.

16. Department of Public Safety / Driving Records

Through the NCIC/CJICS terminal this agency also has ACCESS to the South Carolina Department of Public Safety/Drivers' Records. These records are considered criminal history information and should be treated as confidential data. All other information received through the Department of Public Safety or the Department of Revenue's Motor Vehicle Services should be treated with limited dissemination. Any request from an individual for information concerning a vehicle license tag of a vehicle they may be having trouble with (blocking them in, parking in their yard) should be denied. The use of this file is limited to law enforcement or investigative purposes.

17. Adding and Deleting Certified Operators

a. The terminal Agency Coordinator (TAC) or Assistant Terminal Agency Coordinator (Asst. TAC) will send the following mandatory forms to SLED Quality Assurance Unit via U.S. mail or fax.

* SLED CJIS-NICI Terminal Operator Add/Modify/Delete form
* Third Party Client Application Form

b. The process for completing the addition or deletion should be as follows:

* An operator will be added within (5) five days after NCIC Certification (40 hrs class instruction)
* An operator will be deleted within (5) five days of departure from the Department.

N. Facility

1. Building Security

   a) Front Doors: The front door will be unlocked for public ACCESS Monday - Friday (except holidays) from 0700 to 1700. The door will be locked with a magnetic lock during all other hour communications personnel will allow entry only after proper Identification and need for ACCESS has been determined.

   b) Rear doors: The rear door will remain locked at all times. Departmental personnel will have 24 hour ACCESS through the rear using their ACCESS card.

   c) Communication Center Security

      1.) The Communication Center will be locked using a card ACCESS system at all times. The entrance to the Communication Center will be monitored by a close circuit television. Communication personnel will allow ACCESS to the Communication Center only after visually verifying the identity of the person requesting ACCESS. Only personnel authorized by the Chief will have ACCESS. (CALEA 81.3.1.a). Only authorized personnel will have access to physically secure non-public locations. The MUSC Public Safety Department will maintain and keep current a list of authorized personnel. All physical access points into the agency’s secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logistical and electronic breaches. All personnel with CJI physical and logistical access must:

         a. Meet the minimum personnel screening requirements prior to CJI access.

            i. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
ii. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

iii. Prior to granting access to CJI, the [agency name] on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.

iv. Refer to the CJIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.

b. Complete security awareness training.
   i. All authorized MUSC Public Safety Department, Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.
   ii. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum.

c. Be aware of who is in their secure area before accessing confidential data
   i. Take appropriate action to protect all confidential data.
   ii. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

d. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
   i. Report loss of issued keys, proximity cards, etc to authorized agency personnel.
   ii. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the [agency name] POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.
   iii. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. See Disciplinary Policy.

e. Properly protect from viruses, worms, Trojan horses, and other malicious code.

f. Web usage—allowed versus prohibited; monitoring of user
activity. (allowed versus prohibited is at the agency’s discretion)

g. Do not use personally owned devices on the MUSC Public Safety Department computers with CJI access. (Agency discretion).

h. All others must have a visitors badge or valid identification card and be escorted when in the Communication Center. A visitor is defined as a person who visits the MUSC Public Safety Department facility on a temporary basis who is not employed by MUSC Public Safety Department and has no unescorted access to the physically secure location within MUSC Public Safety Department where FBI CJI and associated information systems are located. Visitors shall

i. Check in before entering a physically secure location by
   i. Completing the visitor access log, which includes name and visitor’s agency, department or company, purpose for the visit, date of visit, time of arrival and departure, form of identification used to authenticate visitor.
   ii. Document badge number on visitor log if visitor badge issued. If MUSC Public Safety Department issues visitor badge, the visitor badge shall be worn on approved visitor’s outer clothing and collected by the agency at the end of the visit.
   iii. Planning to check or sign-in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other that each has their own individual perimeter security to protect CJI.

j. Be accompanied by a MUSC Public Safety Department escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and say CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

k. Show MUSC Public Safety Department personnel a valid form of photo identification.

l. Follow MUSC Public Safety Department policy for authorized unescorted access.

m. Not be allowed to view screen information mitigating shoulder surfing.

n. Individual not having any legitimate business in a restricted area shall be courteously escorted to a public area of the

POLICY AND PROCEDURE # 64
facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, worn personnel shall be notified.

**o. Not be allowed to sponsor another visitor.**

**p. Not enter into secure area with electronic devices unless approved by MUSC Public Safety Department Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the MUSC Public Safety Department assigned personnel.**

2) The call taker station is a backup dispatcher station. The 800mz portable radios are available for joint agency communication as a backup radio communication system in the event of the loss of the master station. **(CALEA 81.3.1.c) (CALEA 81.3.4)**

3) No equipment will be removed from the Communication Center without proper authority. Any equipment being removed will be documented on the appropriate state property control document. **(CALEA 81.3.1.b)**

4) Power sources and transmission lines will be located inside the public safety building with restricted ACCESS monitored by a camera. **(CALEA 81.3.1.d)**

5) Antennas are located on top of the Public Safety Building with ACCESS restricted by an exterior secured ladder. A repeater is located on top of the Basic Science building with ACCESS restricted to physical plant employees and controlled by locked doors. **(CALEA 81.3.1.d)**

**Q. Emergency Power**

The communication center is connected to the building's emergency power generator. The University physical plant personnel are responsible for the maintenance of the generator and do conduct monthly maintenance checks of the generator. **(CALEA 81.3.2)**

**P. Joint Agency Communications (CALEA 81.3.4, 81.2.5.d,)**

The Communication Center will have a portable 800 MHZ radio and a mutual aid radio that will allow them to communicate with local police and a other emergency services departments.

**POLICY AND PROCEDURE # 64**
Q. Radio Outage:

In the event that radio communications is down, cell phones may be used. (CALEA 81.2.10)

DEFINITIONS

AKA: Names other than the name used to make an entry into NCIC that a person may use. This does not include nicknames.

ALIAS: See AKA.

CCH: Computerized Criminal History.

CHRI: Criminal History Rap Sheet

CJICS: Criminal Justice Information Computer System (SLED).

CTA: Control Terminal Agency.

CTO: Control Terminal Officer.

DOE: Date of Emancipation for a juvenile.

DOT: Date of Theft.

DOW: Date of Warrant.

EXTR: Extradition.

FBI: Federal Bureau of Investigations

HIT: A positive response from an inquiry into the NCIC/CJICS terminal.

NCIC: National Crime Information Center.

NLET: National Law Enforcement Telecommunications System.

OAN: Owner Applied Number

OCA: Incident Report Number of Originating Agency.

ORI: Originating Agency Identification Number.

SLED: South Carolina Law Enforcement Division

TAC: Terminal Agency Coordinator

TID: Terminal Identifier.

YR: Ten minute 'hit' response message.

YQ: Ten minute 'hit' inquiry message.

Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the MUSC Public Safety Department for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency’s compliance with FBI and state CJIS systems policies.

Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Agency Coordinator (AC)
An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the MUSC Public Safety Department. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

CJIS System Agency Information Security Officer (CSA ISO)
The CSA ISO shall:
1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA’s user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

Information Technology Support
In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the MUSC Public Safety Department by performing the following:
1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the MUSC Public Safety Department. For agencies who submit fingerprints using Live
Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.

2. Be knowledgeable of required the MUSC Public Safety Department technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.

3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.

4. Properly protect the MUSC Public Safety Department’s CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).

R. Call Boxes

Call boxes are primarily for, but not restricted to students, staff and faculty. Anyone in the area of the boxes that may need help for routine or emergency situations can use the call box to contact Public Safety.

1. Receiving a Call from Call Box

When a call is activated by the call box to the Dispatcher, the voice option will identify in a recorded voice on channel (3) three as well as the central display, identifying the box number. (CALEA 91.1.9.a) The Dispatcher then answers the call and determines what is needed by the caller. The Dispatcher then dispatches an officer to respond to the call box location. (CALEA 91.1.9.c)

2. No Response from Call Box

Should the button be depressed and held in by someone and no conversation takes place, the Dispatcher will immediately dispatch an officer to check the call box location. (CALEA 91.1.9.c)

3. Reset After Call

Press & hold PTT, then transmit the three- digit call box ID number plus the # key sequentially, then release the PTT, or simply let the call box timer automatically reset to standby mode after the programmed amount of time.

4. Low Battery

Should a low battery problem develop, a Dispatcher will send an officer to that location to replace the batter, then test the unit.
S. Card Access

The Dispatcher are responsible for the following duties concerning Card Access:

1. Deactivating Access Cards (Refer to Policy & Procedure # 82 Card Access)
2. Manually Opening Doors (Refer to Policy & Procedure # 82 Card Access)
3. Manually Opening Doors for extended periods of time (Refer to Policy & Procedure # 82 Card Access)
4. Manually Closing Doors (Refer to Policy & Procedure # 82 Card Access)
5. Acknowledge & Resolution of Alarms (Refer to Policy & Procedure # 82 Card Access)
6. Record Activities in CAD Systems (Refer to Policy & Procedure # 82 Card Access)

T. Closed Circuit Television Operations

The installation of the Closed Circuit Television system gives the Department a “tool” to effectively increase our capability and productivity.

1. We have the capability to monitor most of the exterior areas of the campus. Although we have the capability to see most of the campus, the only pictures that are being recorded are the areas that the cameras are actually looking at. (CALEA 91.1.8.f)

2. There usually will not be any strict guidelines on where cameras should be located, but it is incumbent on the Dispatcher, to position all of the cameras to areas subject to the greatest threat. At certain times, direction may be received to keep certain cameras trained at certain locations. (CALEA 91.1.8.f)

3. Certain incidents should trigger an automatic response from the Dispatcher. Some of these events may be:
   a. To monitor an officer during a Terry stop.
   b. The scene of an accident
   c. Elopement from the hospital
   d. Call box activation
e. Card access violation
f. Suspected threat to a facility
g. Code 500
h. Code Red
i. Arrest on the Street
j. Transporting of a Prisoner

4. When the Dispatcher notices an item of interest, he/she should put the applicable camera on monitor four. This will automatically put the image on the monitor at the dispatch station.

5. Dispatchers should alert officers for traffic problems and direct them as required.

6. Night Time Operations – The exterior cameras have excellent night time vision. However, this capability is limited to a small area. It is therefore very important to very carefully select your night time locations, as a large panoramic shot will be of little value. To maximize night time effectiveness, the Dispatcher may be required to adjust the camera iris to obtain the best presentation.

7. Actual equipment operations are covered in the CCTV notebook located on the CCTV console.

8. In case of a call box activation, the Dispatcher should position the nearest camera to that location. A list of the call boxes and the associated cameras and presets are located in the CCTV notebook.

9. As other law enforcement agencies become aware of our capability, it is reasonable to expect specific requests to monitor / tape areas near our campus and within the range of our cameras for use by these agencies as they see fit. Requests such as these should be reported to the Operations Support Commander so that we can accommodate said requests as expeditiously as possible.

All Dispatchers are required to be able to conduct the following CCTV operations:

a. Quickly select the appropriate camera to view a requested area of the campus.

b. Maneuver the camera to get the best picture of the requested area.

c. Adjust the camera iris and focus controls to obtain the best presentation.
d. Demonstrate the ability to use the pan, tilt and zoom capability for fixed cameras.

e. Explain the use of the camera presets

f. Demonstrate the operation of camera presets to locate an Emergency Call Box.

g. Playback a DVR disc.

U. Pawn Pager

The 800 mhz pager alerting warning network (pawn) will consist of radios and pagers distributed to key communications centers within the warning system. This will accelerate to distribution of the emergency message to the emergency responders and facilities within the county. The broadcast channel for this system will be “800 PAGING”.

To activate the system, the Primary Warning Point, Sheriff Office will automatically activate the PAWN for the following situations:

1. Tropical Storms/Hurricane watches and warning OPCON 1-5
2. Tornado Watches and Warnings
3. Mass Fatality/Casualty Incidents
4. Severe Thunderstorm Warnings

PAWN will be activated upon approval of EPD duty officer for the following situations:

1. Severe thunderstorm watches
2. Winter storm warnings
3. Hazardous materials incidents affecting off site areas of a facility
4. Activation of emergency services for disaster situations such as transportation accidents or natural disasters involving mass casualty
5. As required by other agencies.

Secondary Warning System

Should the PAWN system fail for any reason, the warning will be sent via the back up plan using the telephones.

Weekly PAWN Test

The test is conducted every Wednesday at 1300 hours. This is only a test for the pager holders to ensure the pager works. No notification is required to other agencies. Tests will not be conducted if we are already in a server weather watch warning condition.
Alert Checklist

After any “Actual Alert” or “Drill Message” an alert check list will be completed.

V. TDD (telecommunication device for the deaf) (CALEA 81.2.1)

A TDD (telecommunication device for the deaf) is a device that enables people who are deaf, hard of hearing, or speech-disabled to use the telephone by typing messages back and forth to one another instead of talking back and forth. In order to communicate, a TDD is required at both ends of the conversation, unless the call is placed through Relay.

TDDs are traditionally used in one of two ways: either by placing a telephone handset in to the TDD’s acoustic couplers (acoustic) or by directly connecting the TDD to an analog telephone line (Direct Connect). This agency utilizes the acoustic system. The operation and procedure manual is located in the Equipment Manual Binder located in the dispatch center.

W. S.C. Information Exchange (SCIEx)

South Carolina Information Exchange (SCIEx) is a restricted information system for official law enforcement use only. Access is controlled and restricted to authorized users. It is used to support investigative operations, send notification, alerts and provide an avenue to access other law enforcement resources.

It does not take the place of NCIC but enhances the information gathered from NCIC in investigation of criminal activities.

1. Participation:

   In the interest of growth and overall utility of SCIEx, two levels of participation are established:

   Contributing Agency is an agency that contributes information from their RMS, through the agency interface agent device, to the central database for access and use of all participating agencies.

   User Agency is an agency that does not contribute information from their RMS to the central database but is provided access to query the central database.

   At this time MUSC Public Safety Department is a User Agency.

2. Security Policies:

   POLICY AND PROCEDURE # 64
User Access Control - Each user category provides different privileges and functionality. It will require a unique user name and password.

Agency Administrator – Ability to maintain user accounts for a given agency and to update Agency’s data on the SCIEx central server.

Agency User – Ability to perform searches using the preformatted queries.

Agency Administrator Accounts – The Chief of each participating Agency Administrator agrees to appoint, in writing, an Agency Administrator for the SCIEx system. It is recommended that the agency appoint a primary and one backup for this level of authorization. Each agency Administrator is to be assigned a unique account name and password. Agency Administrator account privileges include the name query operation, the ad-hoc query operation and the Agency Administrator interface. The Agency Administrator assigns and maintains all other accounts for that participating agency. Only the SCIEx System Administrator can activate/deactivate accounts at the Agency Administrator level. The SCIEx System Administrator will act only on the written directive of the Chief of the participating agency.

The administrators for the MUSC for the MUSC Public Safety Department are as follows:

Angela Taylor-Batiste

Agency User Accounts – Only the corresponding Agency Administrator assigns Agency User accounts. Each Agency User is to be assigned a unique account name and password. Agency User accounts provide privileges only for the query operations. Agency User accounts are to be deleted by the Agency Administrator once the account is no longer required.

MUSC Public Safety Department will assign all Communications Specialist III (dispatchers) and Investigators as users.

MUSC Public Safety Department SCIEx application form (PSD-183) must be completed by each user.

MUSC Public Safety Department User will be deleted within 5 days of departure or change of position.

Password – Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of SCIEx entire corporate network. As such, all personnel are
responsible for taking the appropriate steps to select and secure their passwords.

MUSC Public Safety Department will require passwords to contain eight alphanumeric characters long including a digit, both upper and lower case characters and punctuation or special character.

Purpose – The SCIEx system will be use as an investigative tool to contain additional information. The following forms will be used for the system in order to maintain an audit trail.

* Request for SCIEx On Line (PSD-182) must be completed and signed by the requesting officer.

* SCIEx Log (PSD-179) must be completed by Dispatchers.

X. MUSC Alert System

In the event that the University needs to be made aware of an emergency, refer to Policy and Procedure # 109 “Emergency Notification System”. The MUSC Alert Manual (red binder) is located in the Dispatch office for instructions.