G.O. Number: 33.2	**Subject:** Communications – Operations
Chapter: 33 Communications	Number of Pages: 45
CFA Standard(s): 25.02, 25.03M, 25.04, 25.05, 25.06, 25.07, 25.08, 25.09, 25.11M, 25.12, 25.13M, 25.14M, 25.15M, 25.16, 25.17M	**Effective: 07/31/2011**
By Order of Chief of Police: Rene G. Landa Chief of Police	**Revised:** 10/18/2023 **Status:** Revised

SECTIONS:

RESCINDS: All existing orders in conflict.

PURPOSE: To establish departmental policy and provide guidelines and procedures for the daily operations of the South Miami Police Department Communications Center.

SCOPE: All departmental personnel. NOTE: If sworn personnel are temporarily assigned to the Communications Center for break relief they will be classified as Communications Personnel and as such, be responsible for the procedures set forth herein.

POLICY: It is the policy of the South Miami Police Department to coordinate along with the Miami Dade Police Department with requests from the public and Department employees utilizing radio, telephone, and mobile digital commutations equipment.

The South Miami Police Department Communications Center provides a 24-hour, seven-days-a- week communications system between the public, the police department, and all uniform patrol officers. Employees should be aware that these policies and procedures are intended as a guideline to employees and do not always provide a solution to every operational question. Therefore, in situations not covered by specific instructions, decisions made and actions taken must be governed by common sense and judgment on the part of communications personnel, or consultation with supervisors.

The Miami Dade Police Department is contracted by the City of South Miami for the primary responsibility of police communications for the South Miami Police Department. Additionally, they have interface capabilities with all state law enforcement agencies and law enforcement agencies in Miami Dade and Broward County if needed. These responsibilities include but are not limited to:

a. **Handling 911 related emergency calls from the City of South Miami and dispatch duties for those calls to all officers in the police department.**

b. **Recording all incoming 911 calls and all police dispatch transmissions on designated talk group frequency.**

c. **Emergency first-aid instruction.**

d. **Interpretation services for non-English speaking persons and/or non-speaking/deaf persons (TDD/TTY System).**

33.2.1 24-HOUR TELEPHONE SERVICE

A. Twenty-four-hour telephone service to the South Miami Police Communications Center is available to the public within the service area of the South Miami Police Department at no cost to the caller.

B. All **9-1-1** emergency calls made from a telephone or cellular telephone within the City of South Miami boundaries are forwarded directly to the Miami-Dade Police Communications Center and answered by a Miami-Dade Dispatcher, twenty-four (24) hours a day. An emergency call is a request for police, fire or rescue services when there is a fire, present or potential danger of injury or threat to life. Some examples of emergencies are: in-progress robberies, a fire, a crash with injuries, a heart attack, someone being assaulted or any crime where the offenders are still on the scene.

C. For non-emergencies, all local residents and citizens within Miami-Dade County may call **(305) 663-6301** to contact the South Miami Police Department Communications Center twenty-four (24) hours a day. A non-emergency is a call for police or rescue services when there is no immediate risk of injury or threat to life. Some examples are: parking violations, a traffic crash without injuries, an abandoned car on the side of the road, a barking dog, a burglar alarm ringing, or other similar calls.

D. For deaf and hearing impaired callers, the South Miami Police Communications Center utilizes a TDD system through the Miami Dade Police Department 911 Center. Calls are received through the Deaf Service Bureau's TDD number and transferred to the Miami Dade Police Department. If a call is received from a hearing impaired person with a TDD/TTY system, complete the following step:[CFA25.02]

    1. Dispatcher will transfer the call to Miami Dade Police Department 911 Center.

33.2.2 SINGLE EMERGENCY NUMBER

A. The Miami-Dade Police Department Communications Center utilizes its own 9-1-1 computer enhanced emergency call system. A South Miami resident, business and/or customer, and cellular phone user within the City of South Miami jurisdiction, in need of help need only dial **9-1-1** on any phone to obtain emergency assistance. The caller's location is automatically displayed on a computer screen when the 9-1-1 call is received.

33.2.3 CONTINUOUS, TWO-WAY CAPABILITY

A. To provide a measure of safety and security to members of the department and the public, the South Miami Police Department maintains 24-hour, two-way radio communications between the Communications Center and officers on duty. [CFA 25.17M]

B. EMERGENCY BUTTON: All portable radios are equipped with a **red** emergency button. Personnel are to use this feature only when their personal safety is at risk or when in need of immediate assistance due to a crime in progress.

1. When the button is pressed, the emergency feature will activate a message which will be visible on all radios tuned to that channel.

2. If it is an emergency, the officer will announce their location and problem, if possible. The Miami-Dade dispatcher will attempt to raise the unit that is checked in under that LID if no immediate response was heard.

3. In the event that the emergency button was activated accidentally, the employee will notify the MDPD Dispatcher immediately and reset the radio by turning the radio off and then back on again.

C. Issuance of permanent radio equipment:

4. Authorized full-time personnel, including all sworn members, shall be issued portable radios and chargers.

5. New police employees will receive their radio equipment fromthe Communications Supervisor.

D. Care and responsibility for radio equipment:

6. Personnel will be held individually responsible for the care and maintenance of issued radio equipment. Negligent loss or damage to radio equipment may result in disciplinary action.

7. Upon separation of employment, the member/employee will return all issued radio equipment to the records custodian, along with other department issued equipment.

33.2.4 RECORDING INFORMATION

A. Dispatchers shall record information on logs and input such as directed by the Communications Supervisor.

33.2.5 RADIO COMMUNICATIONS PROCEDURES

A. In order to eliminate the need for undo repetition of communication messages, voice transmission should be made with maximum articulation. When keying the microphone, the officer should wait two (2) seconds before speaking, otherwise the first few syllables will not transmit. Keep the microphone approximately two (2) inches from the mouth. Speaking too closely to the microphone or holding the microphone too far from your mouth will cause the voice to be unintelligible. The transmission should be brief, accurate and contain specific information.

   1. All primary frequency radio transmissions will be recorded in-house. (MDPD records all frequencies).

   2. The radio is not an appropriate medium for personality conflict, arguments, debate or sarcasm.

   3. Profane and obscene language is illegal and against FCC regulations.

B. Officers will be trained in radio protocol during the basic and field training phases. Training will cover procedures on the necessity of transmitting their location, their status, the nature of cases and any developments in an investigation. [CFA25.09M(a)] Officers will in every case communicate with a dispatcher upon arrival at the scene of an incident, before they leave their patrol cars, when they make vehicle or pedestrian stops and to call in and out of service. [CFA25.09M(b)]

   Transmissions between officers will be only for the purpose of conducting business, and they will be concise, professional, and use a minimum of air time. All initial transmissions will include the sending unit's assigned call number.

   The dispatching of calls for service is done by the Miami-Dade Communication Bureau and is governed by the policies of that agency. They will check on the status of officers on calls if after fifteen minutes there has been no contact with the officer. SMPD Communications personnel and police officers will be mindful of that rule in order to assure officer safety. [CFA25.09M(f)]

   1. <u>In-Service</u>: Officers will advise dispatch that they are "new crew" in- service using their assigned unit number, LID number, and appropriate code (09) when reporting on the air for duty, from a call, a break, or other activity. [CFA25.09M(c)]

2. Responding Units: Responding units will acknowledge the transmission from the Communications Center over the radio and report the location that they are responding from.

3. Arrival: Units will report to the dispatcher by advising their unit number and verbally announcing "arrival" upon the arrival at an assigned call.

4. Dispositions: Dispositions will be given to the dispatcher at the completion of each call or assignment (report or no report).

C. Calls for uniform units will be dispatched in the following order:

a. FTO unit, regardless of assigned zone;
b. Zone Unit;
c. Unit from an adjacent zone;
d. Closest unit from a non-adjacent zone;
e. Shift supervisors may be assigned as a backup unit or primary, if necessary.

Order of Calls Dispatched:

a. Emergency calls for service, whether medical or criminal;
b. In-progress crimes, offender on scene, violent customer disputes;
c. Silent or audible alarms;
d. Non-criminal calls with potential for harm (i.e. vicious animals);
e. Suspicious persons or vehicles;
f. Criminal acts already occurred (i.e. burglaries, auto thefts, etc.);
g. Traffic issues (vehicle crashes, speeders, obstructing traffic, etc.);
h. Noise complaints (barking dogs, loud parties, etc.);
i. Illegally parked cars and all other calls.

D. Q Signals**:** Departmental personnel will use these codes to communicate over the radio frequency to make their radio transmissions brief and moreefficient:

QSL -Do you receive me? Okay; Affirmative.
QTR -Time.
QRU -Are you okay? Is it safe? All is clear.
QSM -Repeat the transmission.
QTH -Location.
QSK - Proceed with your transmission.
QRM - Repeat - I have interference.
QRX - Stand by.
QSY - Change frequency/channels.
QRR - Call for assistance.

Phonetic Alphabet**:** The standard International Phonetic Alphabet adopted by the Association of Public Safety Communications Officers (APCO) will be used by the Communications Center. When it is necessary to spell out words or otherwise use letters in radio transmissions, the following phonetic code words are to be used:

(A) Alpha
(B) Bravo
(C) Charlie
(D) Delta
(E) Echo
(F) Foxtrot
(G) Golf
(H) Hotel
(I) India
(J) Juliet
(K) Kilo
(L) Lima
(M) Mike
(N) November
(O) Oscar
(P) Papa
(Q) Quebec
(R) Romeo
(S) Sierra
(T) Tango
(U) Uniform
(V) Victor
(W) Whiskey
(X) X-Ray
(Y) Yankee
(Z) Zulu

Communications Signal Codes**:** The Miami-Dade County signal codes will be utilized by all personnel on the radio.

E. Communications Center Personnel will monitor the Kendall talk group radio frequency at all times. Dispatchers can communicate with the officers on car-to-car channel "SMPD". South Miami Police Department dispatchers will identify themselves as: **"**South Miami 50**"** and relay their request to a Miami-Dade dispatcher. To obtain priority on the Miami-Dade frequency, the dispatcher will announce **"**South Miami 50, priority**".**

F. Generally, only one officer will be dispatched to handle routine calls for service.

The nature of some calls, however, may require additional officers for safety as well as effective handling of the situation. Additional officers dispatched are to make themselves available for calls when it has been determined that their presence is no longer required. A minimum of two officers will normally be dispatched on the following calls (FTO units count as one officer): [CFA25.09M(e)]

1. Officer assault;
2. On-scene arrest for a felony or violent misdemeanor;
3. Where resistance to arrest is encountered or anticipated;
4. Where use of force is necessary;
5. Crimes in-progress;
6. Civil disturbances or demonstrations;
7. Loud parties;
8. Fleeing suspects;
9. Domestic incidents;
10. Alarm calls;
11. Disturbances and neighbor disputes;
12. Fires;
13. Suspicious persons or vehicles;
14. Whenever assistance is requested by an officer;
15. Whenever a shift supervisor believes additional response is necessary;
16. Whenever the dispatcher believes there will be an officer safety concern. K9 Officers and FTO units are considered to be single officers. The status of the dog is to be disregarded when dispatching officers to 2-man calls. The status of the PPO is to be disregarded when dispatching officers to 2-man calls.

G. Occasionally, circumstances require the presence of a supervisor at the scene of an incident for the purpose of assuming command or in order to assist with the situation.

33.2.6 ACCESS TO RESOURCES

Communications Personnel will have access to various resources to assist them to perform their duties with maximum results and efficiency. Communications personnel will have immediate access to the following departmental resources:

A. On duty supervisor or officer in charge.[CFA25.06M(a)]

B. Duty roster of all personnel, including: [CFA 25.06M(b)]

1. On-call Schedules: On-call schedules are maintained in the

Communications Center for CID and Staff Duty Officers.

2. On-call/Callout requests: When a detective, canine officer or crime scene investigator is needed, notify the on-duty personnel first. If there are no on-duty specialized units available, the dispatcher will utilize the applicable on-call schedule and callout the specialized unit after receiving approval from a supervisor.

C. Telephone numbers of every departmental employee. This information is available in paper format in the appropriate file.[CFA 25.06M(c)]

D. In order to provide for the safety and security of the City, a map of the Department's service area will be available for dispatcher review [CFA25.06M(e)] as well as contact numbers for services external to the police department are frequently required.

1. Dispatchers may directly request assistance from the following list of outside agencies without prior approval: [CFA 25.06M(d)]

   a. Miami-Dade County Fire/Rescue; [CFA 25.07(a and c)]
   b. Miami-Dade County Utilities;
   c. City of South Miami Public Works;
   d. Tow services from the City tow list; [CFA25.07(e)]
   e. Florida Power and Light;
   f. Local telephone services; and
   g. Department of Children and Families (Environmental and human services). [CFA25.07(b)]
   h. Taxi service [CFA25.07(f)]

2. Services that require the notification and approval of a supervisor include, but are not limited to: [CFA25.07(g)]

   a. Florida Department of Law Enforcement (FDLE);
   b. Special tactical teams;
   c. Miami-Dade Police Bomb squad;
   d. Red Cross;
   e. Hazardous materials response team;
   f. Police mutual aid; and
   g. Miami-Dade Police Aviation Unit(aircraft support) [CFA25.07(d)]

E. Tactical dispatching plans: The tactical dispatching plans which include procedures to be followed in directing resources and obtaining information on crimes in progress used by South Miami Police Department communications personnel will be those outlined in the Communications Center Tactical Dispatching Plans for critical incidents and frequently dispatched calls.

1. It is the responsibility of all communications personnel aware of a critical incident to immediately notify the Shift Supervisor.

2. The Shift Supervisor will monitor critical incidents and request additional support personnel if necessary, as follows:

   a. Detectives or K-9 Units
   b. Additional South Miami Police Department personnel, to include:
   c. Assistance from other agencies, to include:

      - K-9 Units
      - Air Support (Helicopter)
      - Additional Road Patrol personnel

3. The Shift Supervisor will determine if notification to the Operations Bureau Captain and/or Staff Duty Officer is necessary.

33.2.7 VICTIM/WITNESS/TELEPHONE CALLS

A. Telephone techniques:

1. Emergency Police Calls: Emergency incidents take precedence over all other calls. Try to keep the caller calm. Reassure them that the police are presently enroute and that additional information may be requested. Continue to gather information about the call, keeping the person talking and act as a facilitator between the caller and responding units.

   a. If the call is a Police Emergency (serious crime and/or in-progress) dispatch the appropriate units. A life threatening in-progress call (robbery, assault, etc.) will be dispatched on a "3" signal (3-29, 3-32, etc.).

   b. Non-life threatening Medical calls, where the caller requests rescue for complaints such as stomach pains, nausea, complaint of not feeling well, sprains, etc., notify Miami-Dade Fire Rescue on a "routine" and dispatch a unit on a "routine" call.

   c. Non-emergency police service calls will be dispatched routine.

2. Attempting to answer all calls within three rings, even if you must place another call on hold momentarily.

3. Communications Personnel will exert every effort to satisfy the needs of the citizens requesting service, assistance, or information and politely

explain those instances where our jurisdiction does not cover. Always suggest alternate procedures or agencies the caller may contact for further information.

4. Communications Personnel answering calls for service will answer the phone by saying, "South Miami Police (give your rank and name)." If another call is placed on hold, or there are multiple lines ringing, ask the caller if they have an emergency. Should the caller reply "yes", find out the nature of the emergency. Should the caller reply "no", answer any other incoming calls in the same manner, placing calls on hold so that the calls can be answered in the order received.

5. Irate and belligerent callers are inevitable when handling a police telephone line. Treat such calls as a challenge, attempting to meet the caller's needs and leaving him/her less upset than they were when they first called.

6. It will be vital that the call-taker get the information from the caller that is appropriate for the call received. If help is being requested, where must it be sent? What type of help is needed? If there is a crime in progress, is there a description of the suspect(s)? The more information Communications personnel can get will only help speed and help make safe the police response.

7. Outgoing telephone calls from the Communication Center are recorded lines and by state law people must be advised they are being recorded. Any employee making an outgoing call from telephone lines within the Communications Center will identify themselves by saying from the outset of the call, "South Miami Police, (rank and name), this call is being recorded…" and then continue with their conversation.

8. In cases where the person being called by one of the outgoing lines in Communications expresses that they do not wish to speak on a recorded line, the employee making the call will inform the person that they will call back on an unrecorded line. Employees can contact the on duty shift commander to use the available Sergeant's cell phone.

B. When a victim/witness calls the South Miami Police Communications Center with a request for information, the dispatcher will inform the caller of the agency's response. If the dispatcher is unable to assist the victim/witness, he/she will refer the caller to a supervisor, police officer, or other person or agency, as the situation dictates.

1. <u>Signal Cancellation</u>: The dispatcher may cancel a signal prior to the unit's arrival if:

a. The complainant advised the Communications Center that a police unit is not required; and/or

b. The incident is not within the City of South Miami jurisdiction.

33.2.8 RECORDING AND PLAYBACK

A. All Communications Center phone lines and radio channels are recorded. This includes incoming and outgoing phone calls. [CFA25.03M] The recordings are kept for a 90 day period, 60 days, plus the minimum 30 days as required by the State of Florida requirements for records retention. [CFA 25.03M(a)]

1. The communications phone recorder is capable of immediate playback for emergency phone call situations and/or investigatory use by departmental personnel. [CFA 25.04M]

2. Immediate radio and telephone playback is available through the Miami-Dade Dispatcher, who is the E-9-1-1 call taker.

3. The SMPD car-to-car channel is recorded by MDPD.

B. The Communications Supervisor is responsible for the daily operation of the communications recorder. The communications recorder and remote terminal are kept securely in the Supervisor's office. [CFA25.03M(b)]

C. <u>Review of Communications Recordings</u>: [CFA25.03M(c)]

1. Police department personnel, with approval of their supervisor, may request recordings of radio or telephone transmissions by completing a written request and forwarding it to the on-duty Shift Supervisor. The Shift Supervisor will sign-off on the request and will forward it to the Records Section.

2. Citizens requesting communications recordings will be asked to submit their requests in writing, including the case number or date and time if possible.

3. The requests will be fulfilled after checking with IA and CID to ensure this is not part of an ongoing investigation.

33.2.9 LOCAL/STATE/FEDERAL CRIMINAL JUSTICE INFORMATION SYSTEMS (CJIS)

A. The South Miami Police Department and its Communications Center have access to the local Miami-Dade County criminal information system, the statewide David information system, Florida Crime Information Center (FCIC) and the nationwide criminal information system, National Crime Information Center (NCIC), retrieving appropriate information from these systems.

B. The Communications Center has a computer terminal giving the department access to FCIC, NCIC, and criminal history files from the Florida Department of Law Enforcement (FDLE). This terminal is utilized in accordance with provisions outlined in the FCIC/NCIC Manual, the FCIC/NCIC User Agreement, and the CJIS Policies and Procedures (see this policy appendix for specifics pg21-39).

C. It shall be the policy of the South Miami Police Department to conform with all rules and regulations as set forth by the Florida Department of Law Enforcement governing the operational use and dissemination of information obtained through the FCIC/NCIC computer system.

1. Only certified operators can utilize the FCIC/NCIC computer. Each operator must successfully complete an FCIC/NCIC certification class. Until certified, the FCIC/NCIC operator must be supervised by a certified operator. Each operator must maintain certification by successfully completing an FCIC/NCIC recertification test every two years.

2. The operator will be certified for full access. Full access certification allows the user to enter, modify, or delete records as well as make inquiries. SMPD enters, modifies, and deletes all records maintained by this agency.

3. The data stored in FCIC/NCIC system is documented criminal justice information and access to that data must be restricted to duly authorized criminal justice agencies. Any information gained through usage of the computer cannot be given to the public. When FCIC/NCIC data is being displayed on departmental monitors and/or terminal screens (including in-car computers), the operator(s) will ensure that unauthorized citizens and the general public are unable to view the information on the screen.

4. Any information obtained from DHSMV (i.e. D/L checks, tag info, etc.) cannot be released to anyone other than police personnel or a criminal justice agency; however, lien holder information can be released to wrecker companies.

5. Criminal history checks can be used for criminal justice purposes **only** (Federal Privacy Act of 1974). Request from non-criminal justice agencies or for non-criminal justice purposes should be directed to the Florida Department of Law Enforcement.

6. All criminal history checks made for another law enforcement agency must be logged in the FCIC Dissemination Log showing dissemination of the check, the subject who was run, for what purpose, for which department, etc. Also, any criminal history printout that is physically given to a departmental employee must be logged in the FCIC Dissemination Log. An audit is done by FDLE once every two years to verify compliance.

7. When the user is finished with the criminal history check, it should be shredded and not retained in case files unless needed for an official investigation. At the end of **each** shift, Communications personnel will shred all criminal history printouts.

8. The South Miami Police Department will investigate any misuse of all protected databases, including the FCIC/NCIC, DAVID, and other DHSMV systems by departmental employees and will take the appropriate progressive disciplinary action, up to and including termination of employment. Violations of these rules can also result in the department's loss of the computer system.

9. All subjects run by officers will be checked via NCIC, FCIC, and Local.

10. No one may be logged on to more than one CJIS workstation at one time. It will be necessary to sign off of one device before logging on to another.

11. Currently SMPD does not allow its members to use personally owned devices to access databases governed by the FBI CJIS security rules.

B. FCIC/NCIC Entries, Cancellations and Confirmations: FCIC/NCIC provides information on active HIT messages; however, information contained in FCIC/NCIC is a tool and does not alone constitute probable cause for arrest or seizure. Follow-up information from the entering agency must be used to verify any HIT.

All hits must be verified by Communications personnel through the entering agency. Upon receipt of a hit confirmation, the originating agency (ORI) of the record must, within ten minutes, respond to the request if it is urgent, and within one hour if its routine. (i.e. a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject).

1. When an officer recovers a stolen item or apprehends a missing person for another agency, the recovering officer must notify SMPD dispatch. The officer will provide the necessary recovery information to the communications officers who will place the necessary locates per FCIC/NCIC policies. Should a wanted person be apprehended, notification to the Miami-Dade Police Department warrants bureau will be made via landline by the arresting officer.

2. If an officer has a stolen item or vehicle to report, or a missing person to enter into the FCIC/NCIC system, the SMPD dispatcher will enter it.

3. All reports and recoveries needing entry into the FCIC/NCIC computer system will be done in a timely fashion.

33.2.10 ACCESS TO INTER-JURISDICTIONAL RADIO SYSTEMS

A. The South Miami Police Department Communications Center is equipped with radio connected to the Miami-Dade Police Department. The South Miami Police Department has the ability to access other inter-jurisdictional systems through the Miami-Dade County radio frequency; MDPD dispatchers have the ability to communicate with other jurisdictions, such as Coral Gables, Miami PD, FHP, and others. [CFA25.09M(d)]

33.2.11 EMERGENCY MESSAGES

A. The South Miami Police Department will assist persons trying to contact relatives, friends, business associates, etc. to deliver emergency messages that meet certain criteria. Criteria to accept such messages include:
   1. Death and fatal accidents;
   2. Critical illness; and,
   3. Check on welfare.

B. Upon the receipt of a death, emergency, or a “check on welfare” notification, the dispatcher will promptly assign an event number to a uniformed officer and give the necessary reference (if the reference is sensitive in nature, the dispatcher will have the responding unit call the Communications Center to receive the information on the call).

   1. If the officer is unable to deliver the notification or message, the task will be reassigned to the next officer working the zone where the notification or message is to be delivered until successful.

   2. As a last resort, a message will be left on the door to have the requested party contact the South Miami Police Department.

C. In the event the South Miami Police Department receives calls to deliver emergency messages that were intended for other law enforcement or public service agencies, the South Miami Communications Dispatcher will relay the message to the proper agency or advise the caller of the correct number for the agency being sought.

D. News Media: This department has a policy to provide the media will all reasonable assistance to do their duty. They may need information regarding situations and incidents that have taken place in the City of South Miami jurisdiction.

1. Any inquiries made by the news media to the Communications Center during normal working hours will be directed to the Chief of Police or his/her designee.

33.2.12 MISDIRECTED EMERGENCY CALLS

A. In the event an emergency call is received by communications unit personnel, the caller shall be conferenced with Miami Dade Police Department's Communications who shall handle the emergency call. Or if an **emergency call** is determined not to be in South Miami's jurisdiction, the dispatcher will transfer the caller by: [CFA 25.05M]

1. First taking the information then transferring the call the Miami-Dade County Communications Center.

2. Any E-9-1-1 calls in Miami-Dade County that are misdirected are re- routed to the appropriate E-9-1-1 call taker by that E-9-1-1 dispatcher (Coral Gables PD, Pinecrest PD, Hialeah PD, Miami PD, &c.)

3. In the event any emergency call ends suddenly (disconnected) and the caller cannot be recontacted, the dispatcher will send two officers to the last known address to check on the caller. The dispatcher will see that responding units have whatever information is available on the call. [CFA 25.05M]

33.2.13 PRIVATE SECURITY ALARMS

The South Miami Police Department does not directly monitor private security alarms. Immediate police response will be provided for all security alarms within the Department's jurisdiction upon notification by an alarm monitoring company or resident.

A. Burglar alarms and Private Security alarms are reported by alarm companies or citizens. If a citizen does not know the exact location of the alarm, ascertain their location and what direction from their location they feel the alarm is coming from.

B. Alarm Complaint Procedure: The Communications Center will determine the nature of all reported alarms that are called in by monitoring companies or

citizens. Communications personnel will also get the following information from the reporter:

1. Appropriate call type;
2. Location of occurrence;
3. Name of the Alarm Company or citizen reporting the alarm, a callback number and the name of the Alarm Company Operator;
4. Business or residence name and phone number;
5. The name, estimated time of arrival, and vehicle description of a responding person, if any;
6. Where the alarm activation is located (window, front door, glass break, etc.) if possible;
7. Alarm Cancellations. Burglar alarms can only be canceled by the monitoring Alarm Company calling back to the Communications Center and only if a South Miami Police Officer has not arrived yet, not by someone at the scene (citizens must call their Alarm Company to cancel if they so desire).
8. Silent Hold Up Alarms will not be cancelled.

33.2.14 REPORTS BY PHONE OR MAIL

A. This Department **will not** take criminal offense reports or non-criminal incident reports, or crash reports that are **not** given in person by a victim, complainant or witness. The Communications Center will not take reports over the phone and will advise complainants that in order for an official report to be filed, it must be written by a South Miami Police Department employee in the presence of the complainant.

B. The South Miami Police Department will accept supplementary information delivered by fax, mail, or telephone interviews for cases that have already been established by an original report, such as new suspect information and Property Loss Reports to supplement stolen item lists. Information will be turned over to the Detective Bureau for the necessary action. Out of state complainants may make reports over the phone.

33.2.15 FIRST-AID INSTRUCTION [CFA25.11M]

A. The South Miami Police Department does not authorize Communications personnel to provide emergency first-aid instruction over the telephone.

B. Communications personnel will follow the established Communications Procedures on handling emergency 9-1-1 calls and will notify Miami-Dade Fire

Rescue on all medical calls, routine and emergency.

33.2.16 LOJACK AUTO THEFT RECOVERY SYSTEM

A. If a patrol unit, operating a vehicle with the in-car LOJACK receiver, receives a "hit" it will appear as an alpha/numeric code number. The code number will be relayed to the MDPD Dispatcher, where Communications personnel will enter the code into the department's NCIC/FCIC data terminal to verify the hit in the FCIC system.

1. The FCIC reply will provide a detailed description of the vehicle which will be transmitted over the radio to the officer by Communications personnel.
2. Any alpha/numeric code beginning with "000" indicates a training code and does not need to be verified through FCIC.
3. The officer will attempt to locate the vehicle using the in-car receiver or advise the Dispatcher of the last known direction of travel.

33.2.17 INTERPRETERS [CFA 25.12M]

A. When non-English speaking person requests police assistance and no one in the Communications Center can assist them, an interpreter may be contacted by transferring them to the Miami Dade Police Department 911 Center.

B. When non-speaking or deaf person requests police assistance and no one can assist them, an American Sign Language ASL interpreter may be contacted through the Miami Dade Police Department (over the radio for in person or via the 911 Center for telephone calls - outlined in 33.2.1).[CFA 25.16]

33.2.18 DISPATCH WITHOUT DELAY

A. Calls will be dispatched without delay, unless unusual circumstances preclude. Calls will be dispatched as soon as possible. The shift commander shall be notified of calls holding.

33.2.19 VALIDATIONS

A. Validation of records entered into both FCIC and NCIC is required and must be completed in a timely manner by the entering agency. This will be completed by a designated Communications Officer on a monthly basis.

To validate a record, the entering agency must check the record for mistakes by comparing the Hot File entry to original and subsequent documentation in the case file. Agencies must also contact the victim, complainant or the court to determine if the record is still active, and this contact needs to be documented in the case file as to how it takes place (e.g. by phone, certified mail, in person or on-line). Once the process is completed, the entering agency may modify information in the record, if needed, and it must include the validator's name.

Invalid records that are allowed to remain in the system could result in a false arrest or a violation of an individual's civil rights. This could further lead to the entering agency being the subject of litigation. The validation process preserves the integrity of the records in the FCIC and NCIC systems.

B. Review the original report and all supplemental reports for accuracy and validity of the entry. The original reports must be used.

C. If a report has reached its retention period and may be destroyed (in accordance with the Division of Archives' records retention rules and regulations) the Services Division Commander will bring this to the Communication Supervisor's or Communications Officer's attention. The report should be reviewed for probability of recovery, prosecution etc. When the determination has been made the entry must be cancelled and the report forwarded to the Services Division Commander for proper destruction.

D. Each record is validated by an attempt to contact the complainant, victim, insurance company or other appropriate source or individual to verify that the person/property is still missing /wanted. This will be attempted by phone or if the phone call is unsuccessful then a departmental form letter must be sent. If the attempt proves unsuccessful then the agency must determine, based on the inability to contact whether or not to retain the record. Once the determination has been made a supplemental report shall be written documenting suchaction.

E. Should the record requiring validation have no supplemental information

available, the detective handling the case or the supervisor for that division shall be notified for follow-up. This is especially important after 30 days for Missing Persons dental records and after 90 days for Missing Persons DNA.

F. Once this has been completed the Communications Officer will be able to electronically validate that record through CJNET with the Florida Department of Law Enforcement.

G. Invalid records that are allowed to remain in the system could result in a false arrest or a violation of an individual's civil rights. This could further lead to the entering agency being the subject of litigation. The validation process preserves the integrity of the records in the FCIC and NCIC systems.

33.2.20 911 PUBLIC SAFETY TELECOMMUNICATOR CERTIFICATION

A. The Miami Dade Police Department has a training program for 911 Public Safety Telecommunicator Certification, to include the following:

1. Certified training provided by the Department of Health (DOH) for 911 Public Safety Telecommunicator; and [CFA 25.17A]
2. Curriculum has been approved by DOH. [CFA 25.13B]
3. Certified/recertified through the Department of Health in accordance with Florida Statue. [CFA 25.14]
4. Certified to provide emergency first-aid instructions over the phone [CFA 25.11M]

B. Miami Dade Communication has certification of all 911 Public Safety Telecommunicator trainees in accordance with Florida Statute, to include the following at a minimum:

1. The trainee must work under the direct supervision of a certified 911 Public Safety Telecommunicator; [CFA 25.15A]
2. The trainee must complete an approved training program and receive 911 Public Safety Telecommunicator certification; and [CFA 25.15B]
3. 911 Public Safety Telecommunicator certification must be achieved within 12 months of assignment. [CFA 25.15C]
4. Miami-Dade established procedures for interpretation services for non-English speakers. [CFA 25.12M]
5. Miami-Dade established procedures for handling calls received through text

telephone(s) (TTY) or Telecommunications Relay Services (TRS). [CFA 25.02] [CFA 25.16]

C. South Miami Police employees assigned to the Communications Unit are encouraged to receive training and become certified through an approved curriculum provided by the Department of Health.

D. Newly assigned SMPD communication personnel will:

1. Complete the approved SMPD communications training program within 12 months of assignment (FTO).

33.2.21 CJIS Policy and Procedure Appendix

South Miami Police Department Policy and Procedures for CJIS Compliance

RELATIONSHIP TO THE FBI CJIS SECURITY POLICY

The overriding goal of this policy is to comply with the FBI CJIS Security Policy and the FDLE User Agreement requirements. Due to the evolving nature of the CJIS Security Policy, it is necessary to separately communicate the requirements of the CJIS Security Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Standard Operating Procedures of the South Miami Police Department. The Agency shall adhere, at a minimum, to the CJIS Security Policy. While the Agency may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy.

PERSONALLY IDENTIFIABLE INFORMATION

Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any NCIC or FCIC provided data maintained by the agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include an individual's PII.

All electronic files that contain PII will reside within the Agency's physically secure location. All physical files that contain PII will reside within a locked file cabinet or room when not being actively viewed or modified. PII is not to be downloaded to workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the Agency. PII will also not be sent through any form of insecure electronic communication as significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted. All disposal of PII will be done by authorized Agency personnel.

All PII will be collected only when there is a legal authority and it is necessary to conduct Agency duties. Access to PII is only conducted when the information is needed to conduct Agency official duties and should only be utilized for official purposes. Agency members will not create duplicate copies of documents that contain PII and will destroy the documents when no longer needed. When PII is extracted from a document Agency members may only target the PII that is required for the task. PII that is extracted shall not be retained beyond the records retention rules for the data and the system it was accessed from. PII shall not be stored or transmitted via personally owned devices. PII may not be taken home by any Agency member.

INFORMATION EXCHANGE

Criminal Justice Information (CJI) is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. CJI is considered any information that is derived from NCIC and/or FCIC and should be treated as such. The Agency will put forth formal agreements with other agencies prior to exchanging criminal justice information as well as the use of a secondary dissemination log. The Agency allows for criminal justice information to be shared with local law enforcement agencies and has current agreements in place with each. This exchange is allowed only via hard copy or electronic copy and will be documented utilizing the agency secondary dissemination log.

Additionally, if the Agency needs to share CJI with another agency that it does not currently have an agreement with, the Agency will verify the person requesting CJI is authorized to receive the information by obtaining their name and contacting the person's agency and verifying they are a current employee. The dissemination will also be documented in a secondary dissemination log. The dissemination log shall include the following information: date, subject's name, SID or FBI number, requestor, requestor agency, operator, reason disseminated, and purpose code.

The agency will validate that the person requesting CJI is authorized to receive CJI prior to disseminating CJI to the requestor. All dissemination logs will be maintained for a minimum of two years.

INFORMATION HANDLING

Information obtained from CJI systems, must only be used for criminal justice purposes. Personnel must follow all CJIS Security Policies and state and federal rules and regulations regarding CJI information. All personnel with access to CJI, audio as well as visual, shall receive the proper training within 30 days of hire (CSP requirement is 6 months). CJI or PII will not be transmitted via email unless it meets the encryption requirements of the CSP. All information outlined in the information exchange and disposal of physical media shall be followed. These procedures shall include all inquiries for both criminal justice and non-criminal justice purposes.

The Agency utilizes servers for storage of criminal justice information. The servers are kept in a CSP defined physically secured location/building inaccessible to non-authorized individuals. The doors have key card locks that are only accessible to Agency employees.

Physical information, such as reports that contain criminal justice information, are stored in the areas and/or rooms that are only accessible to authorized Agency personnel. The documents are stored in locked file cabinets of secured container/room and are only removed when needed for operational purposes. When removed, the information is kept by an authorized individual and then returned. The removal is documented in a log.

All CJI that must leave the facility for transport will be transported by authorized personnel and only for operational purposes.

All computers within the facility shall be positioned in such a way to prevent unintentional viewing or shoulder surfing.

The agency does not allow CJI to be transmitted via email.

INCIDENT RESPONSE for ELECTRONIC and PHYSICAL CJI

For purposes of this policy, an incident is any event that leads to or could lead to the release of CJI to unauthorized people. An incident may involve electronic components used to process, access, transmit or store digital CJI. An incident may also involve the loss of control of physical media including paper documents containing CJI.

To ensure protection of CJI, the agency has created this incident response policy. The policy covers procedures that include preparation, detection, analysis, containment, recovery, and user response activities to an incident as well as the administrative duties of tracking, documenting, and reporting of incidents to the appropriate authorities as required.

AGENCY PREPARATION

The agency has created this Incident Response Policy to prepare for a CJI Security Incident. This policy has been distributed/is accessible to all agency members and will be used as the appropriate procedure in the event of a CJI security incident.

The agency also requires every person that has access to the agency's CJI and/or CSP defined physically secure location to obtain and maintain the appropriate level of CJIS Online Security Awareness training.

REPORTING SECURITY EVENTS

If a security incident occurs involving any device (workstations, smart phones, laptops, tablets, etc.) that is on the agency network, the LASO (Communications Manager) shall be contacted immediately. If a security incident occurs involving any loss of control of physical CJI, the LASO shall be contacted immediately. The LASO will contact additional individuals if the incident requires additional individuals. If it is deemed by the LASO to be a security breach of criminal justice information, a Security Incident Response Form will be filled out and submitted to FDLE Information Security Officer (ISO) at fdlecjisiso@flcjn.net.

All users are responsible for reporting known or suspected information or information technology security incidents. All incidents must be reported immediately to the Agency LASO. The LASO will inform a member of IT and document the incident. When reporting the incident, the user should include all information regarding the incident including any identified weakness associated with the event. If a suspected incident occurs on a user's mobile device, the user shall not turn off the device. The user will leave the device on and report the incident. A member of IT will look over the device and determine if the incident is contained

to the one device or if it is within the Agency system. The agency will employ antivirus on all desktop and laptop devices and will ensure that the antivirus software is up-to-date.

Incident response will be managed based on the level of severity of the incident. The level is a measure of its impact or threat on the operation or integrity of the Agency's information. High Level (potential to impact the network or criminal justice information) Medium Level (potential to impact one system or non- critical system) Low Level (has little or no risk of infecting a criminal justice system).

The Agency will identify the security breach by conducting the following:

1. Confirm the discovery of a compromised resource(s).
2. Evaluate the security incident.
3. Identify the system(s) of information affected.
4. Review all preliminary details. Characterize the impact on the agency as: low, medium, or high.
5. Determine where and how the breach occurred.
    a. Identify the source of compromise and the time frame involved. Review the network to identify all compromised or affected systems.
6. Examine appropriate system and audit logs for further irregularities.
    a. Document all internet protocol (IP) addresses, operating systems, domain system names, and other pertinent system information.
7. Initiate measures to contain and control the incident to prevent further unauthorized access.
8. Document actions throughout the process from initial detection to final resolution.

INCIDENT MONITORING

The LASO and network team will document all security incidents on an ongoing basis and will keep the documentation until it is no longer needed for audits and/or legal action (if warranted).

Reporting Procedures for Mobile Devices

The user must contact the LASO immediately for any incident involving the loss of device, loss of control of the device, or device becoming compromised. The LASO will then initiate steps to resolve the incident and mitigate the risk to the Agency. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the department will use email to expedite the reporting of security incidents.

ACCOUNT MANGEMENT

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

The agency maintains management of all information system accounts to include establishing, activating, modifying, reviewing, disabling, and removing accounts as necessary for each individual. The management of CJI system accounts shall be conducted by Information Technology personnel at the direction of the LASO in accordance with all policies and CJIS Security Policy requirements.

New employee personnel will gain access to all systems upon start date, but will lose access to CJI systems if training courses (Security Awareness, Limited or Full Access Training) are not completed or passed within 30 days (CSP requirement is 6 months). All user accounts of retired, terminated, or otherwise former and non-working employees shall be disabled and revoked immediately or as soon as practical. User accounts suspected of compromise shall be immediately disabled upon first discovery of compromise. Logs of access privilege changes shall be maintained for a minimum of one year. The access level granted to the user for all information systems will be granted based on the satisfactory completion of all personnel security criteria (fingerprint-based background check) and valid need-to-know/need-to-share as required by assignment of official duties.

Account Creation:

1. Upon completion of appropriate state and national fingerprint-based records check, the Agency will notify the LASO and provide the following information regarding the user:
    A. Applicant full name
    B. Applicant date of birth
    C. Applicant social security number
    D. Applicant start date
    E. Applicant assigned MDT (laptop)
    F. Applicant system(s) access
    G. Applicant system(s) permissions
2. The LASO will create and establish a Windows Domain account for the applicant. Each account is uniquely identified by a user name derived from the user's last name followed by the first three letters of the applicants' first name. All accounts are created to ensure a unique username for every individual.
3. The Domain account will be assigned a temporary password and will be set up to require the user to create a new password upon activating the first session. The password for the account must adhere to the Agency password requirements outlined in the Authentication Strategy Policy.
4. The LASO will establish an account for the RMS/MCT and CAD system for the user utilizing the same username requirements.
5. The LASO will identify the level of authority for the user for each application.

A. Officer
B. Supervisor
C. Records
D. User
E. Administrator

6. The LASO will provide the initial credentials and temporary password to the users' supervisor.
7. Upon completion of paperwork, the user will be issued Agency equipment delegated to the users' position within the Agency. Equipment includes, but is not limited to, Agency laptop, MiFi device for wireless access, keys, identification badge and authentication token (grid card) and will sign a receipt for all items. Subsequent equipment changes, deletions, enhancements will be documented via Agency equipment receipt form and approved through Agency chain of command.
8. The LASO will meet with the new user upon starting to ensure proper access to each information system is granted.

Account Modification:

In the event of promotion, demotion, suspension, leave or voluntary or involuntary termination, the supervisor will immediately notify the LASO of the change of status to ensure appropriate access changes are made to systems and applications.

Promotion/Demotion- Supervisor will notify LASO of change of status and change of authority level.

- The LASO will update all systems and applications as necessary to evolve with the current status of employment and will document these changes in the active directory.

Suspension/Leave- Supervisor will notify LASO of the temporary change to the users' account.

- The LASO will temporarily deactivate the account on each system and application.
- The Supervisor will collect all agency equipment from the user and document the transaction.
- Upon reinstatement, the supervisor will notify the LASO and return all agency equipment to the user.
- The LASO will reactivate the user accounts on all systems and applications.
- The user will verify that the accounts are active and sign an equipment receipt.

Account Termination:

- Upon termination from the Agency, whether voluntary or involuntary, the supervisor will inform the LASO of the employment change.
- The LASO will disable all accounts on all information systems and applications.

- The LASO will place the user in the Disabled User Organizational Unit within Active Directory, remove all access of controls from the user, disable Agency e-mail account, and remove remote access ability and all permissions.
- The supervisor will collect all Agency equipment and have the user sign the equipment receipt.

Account Validation:

The LASO will validate Agency User Accounts and Access Privilege Levels at least annually.

- The LASO will document the date and time of the validation on the Agency Validation Form.
- The LASO will verify that all active accounts are current and up-to-date.
- Any changes made by the LASO involving an account will be documented.

SYSTEM ACCESS CONTROL FOR MULTIPLE CONCURRENT SESSIONS

Access control policies are high-level requirements that specify how access to the information system(s) are managed and who may access the information under what circumstance. The purpose of this policy is to define standards and procedures for multiple concurrent sessions within the Agency information system(s).

Access to all CJI systems will be granted by the agency's LASO. Once access is granted, the Information Technology (IT) Department will control access.

Access to Agency information system(s) are based on a user's right to know, authority, and user group.

If the Agency does allow multiple concurrent sessions: The Agency does not allow multiple concurrent sessions within the network except for the following reason:

In Dispatch, the Supervisor may utilize multiple concurrent sessions through RMS for report processing. Once process is complete, they log out of the RMS system.

REMOTE ACCESS

Remote access is any temporary access to the Agency's information system by a user communicating through an external, non-agency controlled network (the internet). Patrol vehicle laptops, satellite offices, off-site IT support, vendor IT support all could be considered remotely accessing the agency's network.

The purpose of this policy is to outline acceptable methods of remote access and the security in place to keep the information system(s) secure.

Remote access shall only be used for official use only. This includes those on duty patrol officers remoting in to agency's network using a VPN tunnel**.** Users may not utilize personally owned devices to access the agency's information system at any time. The agency controls all methods of remote access by only allowing agency approved devices connection through the agency's VPN. All access is monitored by the information technology department and reviewed to ensure proper security protocols are being met. If a user is removed from the agency, the user's access to the information system will be terminated immediately to ensure that remote access is denied.

IT personnel may remote access into the agency's network only for emergency purposes.

Administrative Process for Permitting Remote Access

Prior to establishing the ability for a device and/or a person to remotely access the agency's network, an administrative process to allow the remote access must be completed.

A Remote Access Request form will be completed and signed by a supervisor requesting the remote access privilege. Once completed, the form is submitted to IT to begin technical process of allowing remote access.

Technical Process for Permitting Remote Access

After completion of the administrative process for permitting remote access has been completed, the technical process will begin. The technical process will be completed as follows:

If the remote access will be conducted outside of the agency's CSP defined physically secure location, an approved advanced authentication solution will be implemented on the device.

The device will be configured to use an agency provided virtual private network (VPN) to access the CJI network.

VIRTUAL ESCORTING OF PRIVILEGED FUNCTIONS

Vendor companies may be granted access to the agency's network only if they are virtually escorted by authorized Agency personnel at all times. (If not virtually escorted, the vendor employees must meet all personnel security requirements (fingerprint background check under the agency's ORI), Security Awareness Training level 4, Signed Security Addendums, Vendor contract that incorporates the Security Addendum, and maintain up-to-date records of each vendor employee name, date of birth, social security number, date fingerprints submitted, date of Security Awareness Training and date security

clearance granted. Virtually escorting the vendor employee only removes the fingerprint requirement; all other requirements must be met.)

It is the responsibility of Agency employees, contractors and vendors with remote access privileges to the Agency network to ensure that the connection is secure.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort

2. The escort shall be familiar with the system/area in which the work is being performed.

3. The escort shall have the ability to end the session at any time.

4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.

5. The remote administrative personnel shall be identified prior to access and authenticated prior toor during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

PERSONALLY OWNED INFORMATION SYSTEMS

Personally owned devices are cell phones, tablets or any other device that is owned and maintained by the user, not the Agency.

Personally owned devices are not permitted to access the agency's network. Therefore, a device that is not owned by the Agency, shall not process, store, access or transmit CJI (unless it is an authorized vendor device). Under no circumstances are users allowed to connect their personal device to the Agency network or any other Agency owned devices, applications, or systems.

IDENTIFICATION AND AUTHENTICATION

Identification Policy and Procedures

The Agency LASO will ensure each person who is authorized to store, process, and/or transmit CJI, as well as those individuals who administer and maintain system(s) that access CJI or the CJIS network is uniquely identified by providing the individual with a unique username and password for access to the information system. The creation of the username and password will occur prior to the individual being grantedaccess.

The Agency dictates that each password and User-ID be unique and not be shared with any other individual. Users are forbidden to share their unique password or write it down. All passwords must be memorized.

The Agency ensures that all user IDs belong to currently authorized users and that identification data is kept current by adding new users and disabling and/or removing former users.

Basic Password Standard for Agency's Domain and each CJIS System

All Agency passwords for the Domain and each CJIS System shall meet the following CSP requirements:

1. Be a minimum of eight characters.
2. Not be a dictionary word or proper name. (Must have complexity. For example: the use of upper and lower case letters, numeric characters as well as special characters.)
3. Not be the same as the User ID.
4. Expire within a maximum of 90 days.
5. Not be identical to the previous ten passwords.
6. Not be transmitted in the clear outside the CSP defined physically secure location.
7. Not be displayed when entered.

Authenticator Management

Authenticators will be assigned to personnel during training or upon reassignment. Any lost, compromised, or damaged authenticators should be reported to the IT department immediately. Lost, compromised, or damaged authenticators will be immediately deactivated. To ensure a secure authenticator re-issue process, the user will have to meet in person with the LASO to obtain a new authenticator. Authenticators shall be deactivated immediately if personnel are terminated, retired, or have been reassigned.

Each user that accesses criminal justice information must be uniquely identified prior to being given access to the system and information. The Agency uses standard authenticators (passwords) as well as advanced authenticators (Security Access Card and One Time Password) for accessing criminal justice information in a secure manner.

A temporary standard authenticator is given to the user via the LASO during the first active session the user has. The user then creates a new password that meets the requirements outlined in the authentication strategy policy.

Advanced authenticators are given to users prior to gaining access to criminal justice information outside of the physically secure location. The Agency utilizes Security Access Cards and One Time Password for Advanced Authentication. The LASO will set up individual user access to retrieve the Security Access Card and One Time Password.

Security Access Card and One Time Password Care:

- The user must maintain possession of their access card at all times
- The Security Access card must be stored in a secured area, out of sight from others
- The user shall not share their Security Access card or loan the card to other users
- If the user loses their Security Access card, the user must immediately report the loss to the LASO
- If the user believes their Security Access card has been compromised, the user must report the issue to the LASO

MEDIA PROTECTION CONTROL FAMILY

Media in all forms shall be protected at all times.

MP-1 Policy and Procedures:

PURPOSE: To implement the security control requirements for the Media Protection (MP) control family, as identified in the FBI CJIS Security Policy and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Documented and implemented media protection policies and procedures ensure that access to digital and non- digital media in all forms is restricted to authorized individuals using authorized methods and processes. This policy and the procedures herein must be updated annually and following any security incidents involving digital and/or non- digital media. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

SCOPE AND APPLICABILITY: The procedures cover all Agency information and information systems to include information and information systems used, managed, or operated by a contractor, another agency, or other organization on behalf of the Agency. The procedures apply to all Agency employees, contractors, and all other users of Agency information and information systems that support the operation and assets of the Agency.

BACKGROUND: The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI)

Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

Based on the above outlined requirements and mandates, the Agency is responsible for ensuring the Agency meets the minimum-security requirements outlined in the FBI CJIS Security Policy. All Agency information systems shall meet the security requirements using the security controls defined in the CJIS Security Policy. This document addresses the procedures and standards setforth by the Agency, and complies with the family of Media Protection controls.

PROCEDURES The "MP" designator identified in each procedure represents the NIST-specified identifier for the Media Protection control family, as identified in NIST SP 800-53.

MP-2 Media Access

1. System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non- digital media includes paper and microfilm.
2. The Agency shall ensure that access to digital and non-digital media is restricted to only those individuals with a right-to-know and/or a need-to-know. Access will be based on least privilege and access to systems will only be granted when an account is requested by a users' supervisor.

    a. The Information Technology Team will perform assessment of risk to guide the selection of media for storage, transport, backup, etc., and the associated information contained on that media requiring restricted access.

3. Agency personnel may only use approved Agency removable digital media to store Agency data. The user may request a removable digital device from their supervisor if needed. The removable media shall be encrypted to ensure that sensitive information is secured.

4. Non-digital media shall be restricted to only Agency personnel.
    a. All non-digital media shall be stored securely within the physically secured location. All records will be stored within the records room with access controlled by proximity badges. Non-digital media printed out by users must be stored within the users' desk or filing cabinet.

    b. When removing non-digital media, the records staff will verify the requestor of the record to ensure that the requestor is authorized to access the information. Only approved Agency personnel will be provided the media.

MP-3 MEDIA MARKING

For CJI Information and Information Systems:

1. Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm.

2. The Information Technology Team, in conjunction with the Agency LASO will ensure the following procedures are conducted by Agency personnel in regards to media marking:
    a. Validate that Agency personnel and Information System personnel mark paper and other output products appropriately in accordance with Agency protection requirements, the FBI CJIS Security Policy, and 32 Code of Federal Regulations (C.F.R).

    b. Direct information system personnel and users to adhere to the following when marking documents that contain Criminal Justice Information (CJI)
        i. Mark documents appropriately in accordance with applicable policies and procedures set forth by the Agency so that it is immediately apparent that the information shall be protected from unauthorized disclosure.
        ii. Apply applicable stamps or marks that detail the highest level of protected information contained in the document. Additional detailed information is at the discretion of the agency.
        iii. If a document appears as though it may contain information other than "unrestricted," treat the document as if it is "restricted" until its status can be verified via Agency chain of command.
        iv. If Agency personnel are providing the documents to an approved outside source, such as another law enforcement agency, the user must log the exchange in the Agency's dissemination log. The user must confirm the identity of the requestor prior to providing the information. When providing the requestor, the documentation, the user must stamp the documents as outlined above.
    c. Mark restricted and sensitive information appropriately and clearly.

    d. Mark digital media and cover sheets with the following:
        i. Any applicable security markings such as "i.e. Restricted" is at the discretion of the agency, but must be consistent.
        ii. Mark media to the most restrictive protection level of the information contained on the media.

MP-4 MEDIA STORAGE

For CJI Information Systems:

Note: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper and microfilm). This control also applies to mobile computing and communications devices with information storage capability.

1. The Information Technology Team in connection with the LASO shall:
    a. Physically control and securely store all digital and non-digital media within defined areas using defined security measures.
        i. The agency has deemed that the physical location of the Agency is defined as, and meets the CJIS Security Policy requirements of a Physically Secured Location.

    b. Ensure the assessment of risk guides the selection of media and associated information contained on that media requiring physical protection.
        i. Restrictive information and information systems stored by Agency personnel and contractors shall be physically controlled and safeguarded to the highest level until the media is sanitized or destroyed.

    c. Encrypt data stored on secondary storage devices that reside outside of the Agency's physically secured location. The encryption level must meet the FIPS 140-2 level.

    d. Protect information system media until the media's destruction or sanitization via approved equipment, techniques, and procedures.

    e. Maintain a secure and appropriate facility for archiving digital and non-digital media.

    f. Ensure that only vetted and approved personnel have access to areas and rooms where CJI data and information systems are stored, viewed, and/or accessed.
    g. Physical records must be stored securely.
    h. Retain archived data in accordance with Agency Records Management Policy until the data has reached its end of life and is destroyed or sanitized by Agency personnel.

MP-5 MEDIA TRANSPORT

For CJI Information and Information Systems:

1. The Agency LASO in connection with The Information Technology Team must ensure all information removed from the physically secured location must be protected at all times. Agency personnel are responsible for maintaining control of "CJI" when removed from the Agency.

    a. Guarantee the protection and control of all digital and non-digital media during transport outside of secured locations using defined security measures.

    b. Maintain accountability for information system media during transport outside of the secured location using defined security measures that are agency-approved. For encryption, the product must be a FIPS 140-2 certified encryption technology. The encryption must be controlled by the Agency to ensure total control of the restricted data.

    c. Only authorized individuals may conduct activities associated with transport of information system media

    d. Physical, non-digital media, such as files and documents may only be transported in a sealed envelope and carried at all times by authorized Agency personnel.

MP-6 MEDIA SANITATION

Note: **This control applies to all media subject to disposal or reuse, whether or not considered removable.**

1. Agency personnel and Information Technology staff shall:

    a. Sanitize all information system media (both digital and non-digital) using approved equipment, techniques, and procedures prior to disposal, release out of organizational control or release for reuse by a third-party.
        i. Employ sanitization mechanisms with the strength and integrity commensurate with the categorization for "restricted" information.
        ii. Use sanitization techniques, including degaussing and overwriting memory locations and physical destruction, to ensure that the information on media is not disclosed to unauthorized individuals when such media is reused or released for disposal.
            a. All Agency records shall be properly identified, retrieved from the media, if necessary, and processed in accordance with Agency's retention policy.
            b. Media shall be sanitized using approved equipment and techniques.

iii. Remove all electronic information and licensed software when disposing of computers with hard drives and clean all resources and digital storage of all information.

iv. For sanitizing media:
    a. At a minimum, a 3x technology overwrite method shall be used by the Agency.

    b. The Agency may also utilize a degaussing method to ensure all information has been removed from the device.

v. Hardware Destruction
    a. Only performed by authorized Agency personnel or witnessed by the Agency.

    b. Hard Drives that are physically destroyed need to meet the definition of physically or other methods of destruction, this can be done via drilling holes through the platter.

vi. Physical Media Destruction will occur via an Agency owned cross-cut shredder. The destruction will be conducted onsite by authorized Agency personnel.
    a. For bulk shredding, the Agency will contract with a private vendor who performs bulk shredding while onsite at the Agency. Agency personnel will witness the process from beginning to end.

vii. Ensure media destruction and disposal are:
    a. Performed in a secured environment.
    b. Performed by authorized Agency personnel or witnessed by the Agency.
    c. Undertaken when the information is no longer needed.

MP-7 MEDIA USE

1. Access to the Agency's network(s) and information system(s) may only be provided to authorized Agency personnel.
2. Only Agency provided devices may be used to access the Agency's network(s) and information system(s). Personally-Owned Media Devices and Devices without a known owner shall not be utilized on the network.

3. Agency devices will be provided to Agency personnel only if the user has a need for the technology.

4. Non-Agency issued devices are prohibited from being attached to any Agency device, system, or network peripheral.

5. Logical access to Agency network(s) and information system(s) will be provided via a virtual private network connection approved and provided by the agency.

6. Access Control Lists will be utilized to ensure only authorized Agency personnel have access to Agency information systems and applications.

7. Information Technology will utilize Group Policy to ensure all Agency devices are patched and up-to-date with malware.

8. Physical records will be stored and secured by Authorized Agency Personnel. Only authorized staff will be permitted into where records are stored. Access will be controlled.

PHYSICAL PROTECTION

The purpose of the physical protection policy is to ensure that CJI and information system hardware, software, and media are physically protected through access control measures.

Security Perimeter

The areas where all forms of media are stored are considered a physically secure location. These areas display signs that indicate that only authorized personnel of the agency have access. To ensure the security of the areas, the rooms are only accessible via a proximity card/key/pin access.

Physical Access Authorizations

All individuals that have access to the secure location have been given authorization of entry via a proximity card/key/pin code as well as agency credentials that must be displayed at all times when within the facility.

Access Control for Transmission Medium

All transmission lines within the facility will be secured within the agency to ensure that manual manipulation and tampering cannot occur.

Access Control for Display Medium

All devices that display CJI are positioned in a manner that prevents unauthorized individuals from accessing and viewing CJI.

Monitoring Physical Access

The agency will control and monitor physical access to the server room by only allowing authorized individuals with badge/key/pin access into the room unescorted. All individuals needing access to the area that are not authorized will be escorted at all times by a member of the network team.

Visitor Control

All areas where non-authorized individuals have access will be separated from those areas where CJI is stored, in use, or in transit. Any non-authorized individual granted access to these areas will be escorted at all times by an authorized agent of the agency. The individual will need to provide identification and sign in prior to being escorted within the facility.

Delivery and Removal

Only authorized personnel of the network team are allowed to remove or add information system related items to the network. All items will be brought in or removed by the network team. If an item requires an authorized vendor to perform the work, a member of the authorized network team will escort the individual and witness all work being performed.

ENCRYPTION

Public Key Infrastructure (PKI) Technology - The agency does not utilize PKI.

VOICE OVER INTERNET PROTOCOL (VOIP)

(A) If using VoIP within a network containing unencrypted CJI Voice over Internet Protocol (VoIP) is the routing of voice conversations over a packet switched network as opposed to the traditional circuit- switched telephone network. Voice and data convergence introduces many security issues that must be addressed prior to deployment and use of VoIP technology. The purpose of this policy is to define standards and procedures for the implementation of VoIP telephone systems as well as lay out restrictions in regards to criminal justice information.

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

To ensure the secure environment of the VoIP system, the Agency will enable the underlying data network is configured to host efficient bandwidth and reliability. The VoIP server will be dedicated only for applications required for VoIP operations.

IT will ensure that software patches for the VoIP system and servers originate from the system manufacturer and are applied in accordance with the manufacturer's instructions prior to implementing the patches.

Security:

The Agency will ensure all critical VoIP network and server components are located in the physically secured area and that only authorized personnel have access to them. This will limit physical access to the VoIP network segment.

The Agency will ensure that the default administrative password on the IP phones and VoIP switches are changed prior to implementation.

The Agency will utilize Virtual Local Area Network technology to segment VoIP traffic from the data traffic. The Agency will ensure that the VoIP system is not on the same VLAN as the Agency's information network.

The Agency will use IPsec for all remote management and auditing access of the VoIP system.

The Agency has enabled a VoIP-ready firewall designed for VoIP protocols to aid in securing the system.

VOIP USAGE RESTRICTIONS WHAT ARE THE AGENCY'S USAGE RESTRICTIONS

1. Do not divulge personal or criminal justice information to people you don't know.
2. Be cognizant of discussing criminal justice information using your VOIP Phone on Speaker with unauthorized personnel in the room.
3. Do not install or connect devices to your VOIP Phone such as computers, Bluetooth, recording device,

etc.

4. Do not use mobile software apps to attach to VOIP System.

5. Turn off all unused features on the VOIP System.

6. VOIP phone should not be used for international use (outside the United States and its' territories).

7. Do not store or save criminal justice information on VOIP System.

8. If power is lost to the VoIP adapter or if your internet connection is lost due to a power outage, you will be without phone service. Please ensure that your VOIP Phone is connected to electrical outlet that provides generated power in case of power outage.

9. Do not connect fax machine into VOIP System to fax criminal justice information.

10. Do not connect alarm systems into VoIP System. Alarm Systems must be connected to copper POTS line.

11. If your VOIP Phone System does not provide a dial tone or is not showing the correct time/date and extension, please alert Information Technology (IT) by email, cellular phone or walk-in visit to complete an incident and or work order. The IT department may determine if it is a malicious code (i.e., worms, viruses, Trojans), denial-of-service (DoS), distributed DoS (DDoS), and (though non-malicious) flash crowds event.

(B) The agency does utilize a Voice over Internet Protocol (VoIP) for the telephone system. It is located on its own network and is encrypted.

PATCH MANAGEMENT

All workstations, mobile devices and servers owned by the Agency must have up-to-date operating system security patches installed in order to protect the device and network from known vulnerabilities. Workstations, desktops and laptops have automatic updates enabled for the operating system patches. Current Agency servers have the minimum baseline requirements that define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Agency's data and network.

IT will manage the patching needs for the servers on the network. In addition, they will manage the patching needs for all workstations on the network. IT will routinely assess the compliance of the patching policy and will provide guidance to all personnel of any security and patch management issues. IT also approves monthly

and emergency patch deployments if necessary.

IT will monitor and report the outcome of each patching cycle to the Agency LASO. This will enable the LASO to assess the current level of risk. If a patch is causing vulnerability on the network or appliance, IT will roll the patch back in order to lessen the chance of vulnerabilities on the network. The agency's IT department shall review all security relevant patches, service packs, and hot fixes from the vendors. Once reviewed, the patches will be fixed promptly.

SECURITY ALERTS AND ADVISORIES

Security alerts and advisories are released to IT departments to ensure knowledge of newly discovered threats that may affect Agency Information Systems. The purpose of this policy is to define standards and procedures for security alerts and advisories.

The IT Department will monitor and/or receive alerts and advisories from the locations listed below. If an alert is determined to be critical or pertinent to Agency infrastructure, the appropriate personnel will be notified. All alerts and related actions will be recorded into an information log for Agency records.
The IT department has signed up for alerts and advisories from the following sites:
www.us-cert.gov/ncas/current-activity
https://tools.cisco.com/security/center/publication
https://technet.microsoft.com/en-us/security

1. The Agency will receive information system security alerts and advisories from the above listed sites.

2. Once an alert has been received or detected and has been determined to be a credible threat, IT will notify the Agency LASO. If it is deemed an agency wide threat, the LASO will push the message out to all personnel via internal communications via memorandum or email.

3. IT will take appropriate action depending on the alert. This could include updating security settings and/or issuing information to all relevant Agency personnel with directions to ensure proper handling of the issue.

IT will document the details of the alert in the security incident log. The log will remain with IT for a period of four years.

WIRELESS USAGE RESTRICTIONS/LOGS/MOBILE DEVICES

The Agency has created the policies and procedures for Mobile Devices in an effort to establish usage restrictions and implementation guidance for mobile devices as well as authorize, monitor, and control wireless access to the information system.

WIRELESS USAGE RESTRICTIONS/LOGS

The Agency has implemented a wireless network for ease of daily operations. The use of the wireless network is for Agency information and systems only and should be utilized as such. The purpose of this policy is to provide the requirements for utilizing criminal justice information system(s) with wireless access.

The Agency utilizes wireless access for the ability access the Agency information system. Agency personnel are only permitted to use the Agency wireless network for Agency business. Personnel may only access the network with Agency owned equipment. The IT department will authorize individual users to utilize the network by giving them an agency owned mobile device. The IT department will monitor all connections and audit logs associated with the devices as well as the systems and applications that the device accesses. IT will review these audit logs on a monthly basis or more frequently if there is an increased risk to agency information or systems.

Agency personnel are not allowed to access Agency systems on any public wireless network without connecting to the Agency provided Virtual Private Network for authentication. The access to the information system is only allowed for job-related functions. All personal use is prohibited. Users are not permitted to attempt to add, remove or modify any hardware, software, network devices or other information systems in place within the Agency. If the user requires additional hardware, software, or network devices to perform duties related to their current job function, the user must contact the LASO to request the addition. Once the LASO has deemed the addition as relevant to job functions, the LASO or technology team will conduct the changes to the device.

Reporting Procedures for Mobile Devices

The user must contact the LASO immediately any incident involving the loss of device, loss of control of the device, or device becoming compromised. The LASO will then initiate steps to resolve the incident and mitigate the risk to the Agency. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the department will use email to expedite the reporting of security incidents.

BLUETOOTH

Bluetooth technology is utilized as the open standard for short-range radio frequency communication. This policy provides the minimum baseline standard for connecting Bluetooth enabled devices to the Agency owned devices. The Agency utilizes Bluetooth technologies for operational processes only.

Bluetooth technology, while not as secure as other forms of wireless technology is utilized for operational needs within the Agency. Currently, the Agency utilizes Bluetooth technology with the Rapid ID device. The device relies on Bluetooth due to the ability of the technology to operate in noisy environments by moving from frequency to frequency. By doing this, the device avoids getting interference from other signals as it transmits or receives the identifying information.

The user must only use Agency owned Bluetooth devices to pair with criminal justice information systems. Currently, the user may only use the Rapid ID device for Bluetooth Technology. The Agency maintains these devices and ensures that they meet the minimum requirements of Bluetooth specifications. All other Bluetooth devices are not to be utilized to pair with Agency systems, networks, and hardware.

- The Agency is responsible for maintaining an encrypted security mode between the device and the pair.
- The Bluetooth device must be in hidden mode to ensure that other individuals cannot connect to it.
- The user should only activate Bluetooth when it is needed to perform an identification check
- The Agency must ensure the firmware is up-to-date and that all patches are current

Bluetooth will only be used for official business purposes. The purposes include the agency's Rapid IDs, printers, and wireless mice. All other Bluetooth devices shall be approved by the agency's IT department.

INCIDENT RESPONSE FOR LIMITED FEATURED OPERATING SYSTEM DEVICES

This agency does not utilize Limited Feature Operating System Devices such as I pads, Tablets, cell phones, PDA devices, etc.

PERSONNEL SANCTIONS

Any user who violates any portion of this policy will be subject to the standard disciplinary processes in place with this Agency. Sanctions against staff that violate information systems and or security policies may include formal disciplinary action up to and including termination based on offense severity.