MONROE COUNTY SHERIFF'S OFFICE

General Order

CHAPTER: 052		TITLE: Information Management/Records
EFFECTIVE DATE: December 13, 2012	**NO. PAGES:** 20	**REVIEWED/REVISED:** January 22, 2015
REFERENCE: CALEA 11.4.4, 41.3.7, 42.1.3, 74.1.3, 82.1.1, 82.1.2, 82.1.3, 82.1.4, 82.1.5, 82.1.6, 82.2.1, 82.2.2, 82.2.4, 82.3.1, 92.3.2, 82.3.5, 82.3.6		**RESCINDS:**
Sheriff of Monroe County		

I. PURPOSE: The purpose of this directive is to establish guidelines for the security of Sheriff's Office records and files consistent with public record laws and for the overall operations of the Smart Cop System and Records Section.

II. DISCUSSION: It is the policy of the Sheriff that the Office has a central records section to meet the management, operational and information needs of the Office and to place accountability for the records function in a specific specialized component. This component is more specifically concerned with field reporting and central records activities and is not intended to address the records functions attendant to specialized entities within the Office. The Records Supervisor, who is directly responsible to the Director of Records, supervises the Records Section.

A. The main function of the Records Section is to:

1. Review reports for compliance with directives
2. Control the storage and flow of reports
3. Maintain Office records as specified by law and the Sheriff
4. Retrieve records when necessary or requested

B. Ensure a record is made for each request for service to include:

1. Citizen reports of crime
2. Citizens' complaints
3. Citizen request for services when:

    a. A deputy is dispatched
    b. A member is assigned to investigate
    c. A member is assigned to take action now or at a later time

4. Criminal and non-criminal cases initiated by law enforcement officers
5. Incidents involving arrest, citations, or summonses

C. All reporting carried out as a result of the above shall include:

1. The date and time of initial reporting;
2. The name (if available) of the citizen(s) requesting the service, or victim's, or complainants name;
3. The nature of the incident; and
4. The nature, date, and time of action taken (if not) by law enforcement personnel.

III. POLICY AND PROCEDURES

A. Confidential Records: The Sheriff's Office recognizes that there are types of information contained within various reports generated by the Agency, which are legally confidential. The Office further recognizes and accepts its responsibility to respond to request from the public for information contained in these reports, releasing any information that is legal to release and protecting any confidential information from inappropriate, untimely, or illegal release. The following includes, but is not limited to, information that is confidential and exempt from public inspection and examination as defined by Florida law.

1. Active criminal intelligence information and active criminal investigative information.

2. Information revealing the identity of confidential informants or sources.

3. Criminal intelligence or criminal investigative information that could reveal the identity of the victim of a sexual battery, any sexual offense, including a sexual offense proscribed in chapter 794, chapter 796, chapter 800, chapter 827, or chapter 847 or child abuse as defined by Florida law or a photograph, videotape, or image of any part of the body of the victim of a sexual offense prohibited under chapter 794, chapter 796, chapter 800, § 810.145, chapter 827, or chapter 847, regardless of whether the photograph, videotape, or image identifies the victim, or any information in a videotaped statement of a minor who is alleged to be or who is a victim of sexual battery, lewd acts, or other sexual misconduct proscribed in chapter 800 or in § 794.011, § 827.071, § 847,071, § 847.012, § 847.0125, § 847.013, § 847.0133, or § 847.0145, which reveals that minor's identity, including, but not limited to, the minors' face, the minors' home, school, church, or employment telephone number, the minors' home, school, church or employment address; the name of the minors' school, church, or place of employment, or the personal assets of the minor; and which identifies that minor as the victim of a crime described in this subparagraph, help by a law enforcement agency.

4. Information revealing surveillance techniques, procedures, or undercover personnel of any criminal justice agency.

5. Criminal intelligence or information that reveals the personal assets of the victim of a crime, other than property stolen or destroyed during the commission of a crime.

6. Criminal intelligence and investigative information received by a criminal justice agency prior to January 1979.

7. The home addresses, telephone numbers, social security numbers, dates of birth, and photographs of active or former sworn or civilian law enforcement personnel and the home addresses, telephone numbers, social security numbers, photographs, dates of birth, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel, as well as several other positions please refer to Florida State Statute 119.071. **Please refer to the statute as there are several different occupations covered**

8. The identity or address of a juvenile unless the child is 16 years of age or older and has been taken into custody for a violation of law, which if committed by an adult would be felony, or the name and address of any child 16 years of age or older who has been found by a court to have committed at least three or more violations of law which, if committed by an adult, would be misdemeanor this is in effect only for arrest prior October 1, 1994.

9. In order to protect the rights of the child and the child's parents or other persons responsible for the child's welfare, all records received by Department of Children and Families concerning reports of child abandonment, abuse or neglect, including reports made to the

central abuse hotline and all records generated as a result of such reports, shall be confidential and exempt from the provisions of Florida Statute 119.02 (1) and in accordance with Florida Statute 39.202.

10. Social Security Numbers.

11. A photograph or video or audio recording that depicts or records acts or events that cause or otherwise relate to the death of any human being, including any related acts or events immediately preceding or subsequent to the acts or events that were the proximate cause of death.

12. A complaint of misconduct filed with an agency against an agency employee and all information obtained pursuant to an investigation by the agency of the complaint of misconduct until the investigation has concluded.

B. Responding to requests for information in Police Reports

1. When a member of the public requests information or access to Public Records from any member of the Sheriff's Office, they should be directed to Central Records or the Records Division in each district which is responsible for releasing to the public or making available for public review any information from any Public Record in any form.

2. Requestors are not required to present ID, sign in, "put in writing", or tell you why they want certain documents to make a public records request.

3. Building security policies must be maintained and enforced.

    a. Requestor may use video in our office reception area, however you are not required to consent to the recording of your voice and you are not an authorized agency spokesperson

    b. If you receive a request to inspect or copy records that are easily accessible and you have the time to do so, acknowledge the request and provide the copies if possible. If you are unable to provide copies at that time, allow inspection and advise the requestor when they can pick up the copies. This must be done within a reasonable time. If a request is made to photograph the records, please allow them to do so.

4. If the request is for documents held by the Monroe County Sheriffs' Office at another location, call Central Records. They will assist you and facilitate compliance.

5. Questions concerning the release ability of a record shall be directed to the Central Records Section Supervisor and, if not available, to the Director of Records.

C. Direct Access: The following shall serve as guidelines for direct access to Sheriff's Office records and files.

1. Only Records Division personnel shall have direct access to the Records Section Digital Imaging System files. All other personnel of the Sheriff's Office shall have limited access to records through the SmartCop or PowerWeb system without the help or permission of the Records Section. Access to these records is assigned by the Director of Records and is dependent on the employees job function

2. Only designated District and Central Records personnel are authorized to release records.

D. Duplication of Office Records

1. Office records may only be duplicated for official purposes.

2. Official records or duplications thereof shall not be maintained outside of agency offices.

E. Juvenile Records

1. Electronic juvenile records shall be tagged as juvenile records and are confidential.

2. Paper juvenile files, fingerprint cards and photographs shall be marked "Juvenile Confidential".

3. Fingerprint cards and records relating to juvenile offenders and delinquent children shall not be open for public inspection except as authorized by Florida Statute 985.11, and paper format files shall not be commingled with fingerprint cards and records relating to adult offenders.

4. Records of juvenile offenses once reaching adult age shall remain on file until an Order from the Court allows their removal, per Florida Statute 39.12 (2).

F. Record Expungement

1. Upon receipt of a Court Order to expunge or seal a criminal history record, the Records Supervisor or his/her designee shall initiate the following procedural steps to insure that the requirements of law are met. ALL COURT ORDERS MUST BE CERTIFIED. All court orders must be accompanied by a Florida Department of Law Enforcement certificate of eligibility.

2. Any request for a record that has been sealed or expunged shall be handled directly by the Records Section Supervisor.

3. Expunction or sealing

    a. Identify the subject of the court order with the subject's arrest record, case number, and date of arrest.

    b. Prepare a letter of transmittal citing specific identification of the subject and arrest information to be expunged or sealed. The Sheriff or his designee will sign the letter.

    c. Attach a copy of the Court Order to the letter of transmittal and forward via email. Expungecourtorder@fdle.state.fl.us

    d. Notify all agencies and/or office divisions to which the subjects affected records have been disseminated.

4. Juvenile

    a. Identify the subject of the court order or document requesting expungement with the subject's arrest record, case number, and date of arrest.

    b. Prepare a letter of transmittal citing specific identification of the subject and arrest information to be expunged or sealed. Such letter shall have the signature of the Sheriff or his designee.

    c. Attach a copy of the Court Order to the letter of transmittal and forward to via email. Expungecourtorder@fdle.state.fl.us

d. Notify all Agencies and/or Office divisions to which the subject's affected record has been disseminated.

5. Administrative Expunction: See F.S.S. 943.0581 for the requirements.

   a. How to Complete Administrative Expunction.

   b. The following information must be on Agency letterhead:

      1) State the reason for the administrative expunction
      2) The request must include the following identifying information:
         a) Name and Alias(es)
         b) Sex and Race
         c) Date of Birth
         d) Social Security Number (if available; used for identification – not mandatory)
         e) Date and time of the Arrest
         f) Original Charges
         g) DLE number (also known as State I.D. #)
         h) OBTS number
         i) Must be signed by the Sheriff or designee
      3) Email application to: Qualitycontrol@fdle.state.fl.us

6. All expunged/sealed information shall be taken out of all systems as soon as certified copy of a Court Order has been received.

7. Scanning Expungements: Once you have received proper paperwork to expunge and record has been expunged (in the computer), Central Records will do the following:

   a. Collect all records pertaining to the file
   b. Scan FDLE letter, certificate of eligibility & Court Order in the Fortis Imaging System.
   c. Verify the above listed paperwork has been scanned, is legible, and then destroy the paper documents and or delete computer documents/files.

8. Scanning Sealed Records: Once you have received proper paperwork to seal and record has been sealed (in the computer), Central Records will do the following:

   a. Collect all records pertaining to the file.
   b. Scan all documents along with FDLE letter, certificate of eligibility and court order in the Fortis Imaging System.
   c. Verify all paperwork has been scanned and is legible, then destroy the paper documents and or delete computer documents/files.

9. Scanning Records with Special Circumstances: If there are several suspects listed, but only one person's records are being sealed or expunged Central Records will do the following:

   a. Sealed Records: Once you have received a certified copy of Order to Seal and Certificate of Eligibility from FDLE; Central Records will do the following:

      a) Collect all records pertaining to the file
      b) Redact all required information of the suspect being expunged.
      c) Re-scan; replace the paperwork already scanned, as well as the letter from FDLE, Court Order & Certificate of Eligibility
      d) Destroy all paperwork and or delete computer documents/files.

   b. Expunged Records: Once you have received a certified copy of Court Order and Certificate of Eligibility from FDLE; Central Records will do the following:

a) Collect all records pertaining to the file
b) Redact all required information of the suspect being expunged from the other suspects' records in SmartCop.
c) Re-scan; replace the paperwork already scanned, as well as the letter from FDLE, Court Order and Certificate of Eligibility.
d) Destroy all paperwork and/or delete computer documents/files.

10. The file within the Fortis Imaging system will be restricted to the following personnel.

    a. View Only

        1) Sheriff
        2) IT personnel
        3) Sheriff's Administrative Assistant

    b. View and edit

        1) Central Records Supervisor
        2) Central Records Assistants

G. Field Reporting: Refer to General Operations Manual, Chapter 90 - Report Writing Manual and Smart Cop Case Numbering System.

H. Supervisory Review of Reports

1. It is the responsibility of every supervisor to ensure that incident and traffic reports submitted by subordinates are thorough, accurate, and comply with all policies and procedures by reviewing them prior to final submission.

2. Approving Reports

    a. Each report will be thoroughly read by the reviewing supervisor. The editing supervisor shall insure that:

        1) All appropriate sections, lines or other entry items are correctly completed.
        2) The crime classification is correct.
        3) The body of the report is written in a correct format.
        4) Spelling, grammar, and phraseology is correct and appropriate.
        5) All written items in the report are clear and legible.
        6) Insure that all pertinent information is documented.
        7) Insure that to the fullest extent practical, all leads, clues, or any suspect information is pursued to a satisfactory conclusion.
        8) Ensure that a "good-faith" effort to solve any reported crime is made

    b. When the supervisor determines that an incident report meets each of the investigative and report writing standards set forth herein, the supervisor shall approve the report in SmartCop along with his/her ID number and Sector number.

    c. When a supervisor determines that a traffic report meets each of the investigative and report writing standards set forth herein, he/she shall approve report in Smart Cop.

3. Rejecting and Corrections of Reports

    a. Supervisors shall reject any incident or traffic report not meeting the above listed report writing or investigative standards, and shall:

1) E-mail the member. It is the employee's responsibility to correct the report and e-mail the supervisor of such correction.

2) Corrections of reports shall be accomplished with in twenty-four (24) hours.

b. Supervisors, other than the member's supervisor, who rejects an incident report shall:

1) E-mail the members supervisor that the report has been rejected. The member's supervisor will then forward to the originating member.

2) Members shall follow previously outlined procedures for correcting and advise the supervisor of corrections.

c. Uniform Crime Report (UCR) classification personnel who believe an incident report would be rejected shall notify the appropriate District Commander for review and appropriate action.

4. Routine Reports: Once the supervisor has reviewed the reports, the supervisor will approve all narrative, supplements and then the entire report electronically.

5. Routing Reports

a. Law enforcement supervisors are authorized to review, approve, and or refer reports.

b. Supervisors will also make copies of any supporting documents and route to the referred unit.

c. Original supporting documents will be sent to the Records Section, unless otherwise indicated in the narrative. Supervisors will rout referred reports to the State Attorney's Office.

6. Case Status: Case status shall be determined by the following criteria:

a. All cleared cases shall adhere to the Uniform Crime Report guidelines for case clearance.

b. The judgment of reviewing supervisor shall determine active or inactive status of other cases based upon the fulfillment of the investigative criteria.

c. Correct case status shall be indicated by the U.C.R. clerk by marking the Offense Status field.

1) Cleared by arrest
2) Exceptionally cleared
3) Unfounded
4) Active
5) Inactive

I. Report Distribution

1. Investigative reports: will be distributed by the reviewing patrol supervisor or investigative supervisor. Most reports are in electronic format and may be distributed as such.

2. Supplemental reports: same procedures will be followed as with initial reports.

3. Insurance reports: Approved copies of reports requested by insurance companies will be forwarded within forty-eight (48) hours after the request is received.

4. Media reports: all reports for media purposes shall be released through the appropriate Public Information Officer, unless requested by an individual through the Records Section.

5. Reports involving domestic violence or juveniles shall be forwarded to the appropriate agency or organization within 24 hours after receipt (Domestic Abuse Shelter, FL Dept. Of Juvenile Justice, FL Dept. of Family and Children). The station Commander shall ensure compliance with this policy

6. Criminal Citations/Notice to Appear, DUI Arrest and other appropriate reports will be forwarded to the State Attorney's Office and Clerk of the Court.

7. Fees will be assessed according to the established schedule found in Chapter 52B.

J. Control of Reports

1. Daily Reports

   a. Central Records shall account for all reports by incident number assigned by the Computer Aided Dispatch (C.A.D) System

   b. Supervisors shall ensure all supplemental or handwritten reports are forwarded to Central Records for master control and filing.

   c. Whenever incident reports are assigned, incident numbers are matched to the appropriate report utilizing the C.A.D. report. The Central Records Supervisor shall notify the appropriate Sector Commander of reports not accounted for after three (3) business working days.

2. Follow-up Reports: As follow-up reports on active cases are completed, they shall be forwarded through the chain-of-command to Central Records for scanning into Fortis with the original report. The Sector Records Unit shall maintain all follow-up reports and forward them to Central Records every ten (10) days.

K. Audits

1. Daily: Central Records shall conduct a daily audit of all case numbers drawn each day. This is to insure that all reports and follow up reports are received and accounted for in the Smart Cop system.
2. Monthly: Every record listed in F/NCIC hot files will be validated for accuracy.

L. Scanning Offense paperwork: When any documentation related to an offense is received, it will be scanned in to the Fortis Imaging System.

M. Privacy and Security Precautions for the Central Records Function: No member of the Office or public, except assigned to the Records Section, or those authorized by the Director of /Records, shall be allowed beyond the point so designated.

N. Records Retention Schedule: All records are retained according to the GS1-SL and GS2 which is distributed by the Florida Division of Archives Historical Records Management, which dictates the length of time and the media by which records shall be maintained. No records shall be disposed until written approval has been granted by the agency designated Records Management Liaison Officer. Utilize the “Records Disposition Document” found in the Public Records Folders in Outlook to obtain approval. [CALEA 42.1.3 e]

O. Central Records information shall be available to operational personnel, twenty-four (24) hours a day, seven days a week, in the form of on-line data.

P. Master Name Index: The Records Section shall manage an electronic alphabetical master name index. The criteria for inclusion of names in the index shall be the name of victims, complainants, suspects, persons arrested, witnesses, those receiving a traffic citation or warning, and those for whom a Field Interview Report (FI) was completed.

Q. The Law Enforcement Records Section shall maintain electronically:

1. An index of incident by location
2. An index of incident by type
3. An index of stolen, found, recovered, and evidentiary property
4. A modus operandi file

R. The Corrections Record Section shall maintain: A booking file on each person arrested to include:

1. Updated information obtained from State and Federal rap sheets (i.e. FDLE, FBI and fingerprint classification number)
2. Photograph
3. Copy of Arrest Report

S. All records to be maintained by the Monroe County Sheriff's Office shall be controlled by the Records Section, except as otherwise provided by Office directives.

T. Case Disposition Records: Central Records will be responsible to maintain all disposition forms that were forwarded from the State Attorney's Office.

U. Warrants Section:

1. Main functions of the Warrants Department are:

    a. Enter and maintain accurate wanted persons records.
    b. Control the storage of wanted persons records,
    c. Audit the wanted persons records according to FDLE
    d. Make attempts to locate wanted persons.
    e. Answer Hit confirmation requests within 10 minutes
    f. Prepare documents for extradition of our wanted persons.

2. All warrants and writs directed to be served by the Sheriff of Monroe County, Florida, shall be entered into and maintained in SmartCop by the Warrants Section. [CALEA 74.1.3 c]

3. FCIC/NCIC Entry [CALEA 74.1.3 a]

    a. All such warrants shall then be entered into the FCIC (Florida Crime Information Center & NCIC (National Crime Information Center) computer database.

    b. Felonies: In the extradition limitation section for Felonies with a bond amount less than $5,000.00 it will be noted "Florida Pick-up Only", unless there is a warrant information sheet from the State Attorney's Office or notation on the warrant from the Judge stating otherwise.

    c. Misdemeanors: In the extradition limitation section it will be noted “Florida Pick-up Only”, unless there is a warrant information sheet from the State Attorney’s Office or notation on the warrant from the Judge stating otherwise.

d. Writs

1) Child support writs are eligible to be entered in FCIC only.
2) Other types of writs are not eligible to be entered in F/NCIC.

4. Juvenile Warrants: Juvenile felony and misdemeanor warrants, orders to take into custody and dependency warrants will be entered into the NCIC system.

5. Scanning Warrants and writs

a. Once warrants and writs are entered in the Smart Cop System they will be scanned into the Fortis imaging system.
b. All warrants are available to the operational personnel 24 hours a day, 7 days a week in the form of online data via PowerWeb.

6. Extradition [CALEA 74.1.3 b]

a. Out of State: After a subject is located in another state a copy of the original warrant and the hit confirmation request will be forwarded to the Extradition Coordinator to confirm extradition with the State Attorney Office.
1) If extradition was confirmed by the SAO the Extradition Coordinator will arrange a pick up.
2) If extradition was reduced by the SAO the warrant will be updated with new extradition information in all systems.

b. Out of County: After a subject is located in another county within the State you will verify whether or not subject is going to post bond on our warrant. If subject does not post bond you will forward all information to the Extradition Coordinator to take care of pick up arrangements. If extradition was reduced by the SAO the warrant will be updated with new extradition information in all systems.

7. Warrants or writs from others Agencies: If you receive a warrant from an Agency from another County or State asking us to locate subject because they have information that they are residing in our County. The information is entered into a computerized log. The warrant will be forwarded to the appropriate Substation for service. After an attempt to serve is made the warrant is returned to the Warrants Department with an appropriate notation. The warrant will be returned to the originating Agency.

8. Warrants shall be cancelled for service and recall only. Should a warrant be canceled, notice shall be given to all personnel involved. [CALEA 74.1.3 e]

9. Prior to service of any warrant, verification will be made. [CALEA 74.1.3 d]

a. Local Warrant: As entry in the computer must be verified and must have a physical warrant in file or the scanned document in the Fortis System.

b. Out-of-State and County: Verification must be made with the originating agency by teletype.

10. Canceled warrants/writs will be sent to the Clerk of Courts via courier.

11. Injunctions:

a. All active Injunctions/Protection Orders will be entered/updated in the Smart Cop system within 24 business hours of receiving.

b. All active injunctions will be entered in NCIC.
c. Permanent injunctions will be updated in Smart Cop, NCIC, scanned into the Fortis imaging system and shredded.
d. Dismissed injunctions will be recalled from Smart Cop, canceled from NCIC, scanned into the Fortis imaging system and shredded.

12. 1FDLE audit will be conducted every month on warrants, writs and injunctions entered in F/NCIC to make sure every record is still valid and the entry is accurate.

13. Accurint search is done to locate and arrest people with active warrants or to find deceased people with active warrants

    a. If a person with active warrant is located an attempt to locate and arrest will be sent via teletype.
    b. If a person with active warrant is deceased the warrant(s) will be recalled and sent back to the Clerk of Court.
    c. All attempts to locate will be entered in the computerized log.
    d. The log is posted on the Outlook every month.

14. Warrant Recalls will be done in a timely manner. A recall log book will be maintained by the warrants section. A computerized recall log will be posted in Outlook every business day.

V. Traffic Citation Records & Crash Reports

1. Records retention of citations

    a. All citations and warnings shall be completed in SmartCOP Mobile Forms

    b. All citations and transmittal slips shall be forwarded to the Clerk's Office, by each appropriate District, within five (5) days after being completed.

    c. Copies of citations may be kept by District Records Section.

    d. It shall be the duty of each respective District Commander to ensure the entry of the handwritten Citations and Warning into the Smart Cop system and the transmittals to the Clerk's Office are accomplished.

    e. It shall be the duty of District Records Section, under the direction of the District Commander to audit the information and send back requested changes, to the originating Deputy.

2. Citation Accounting

    a. Paper Citations are ordered from the DHSMV, by the Traffic Unit Supervisor on an as need basis.

    b. District Commanders shall advise the Traffic Unit Supervisor of their need for paper citations.

    c. Paper Citations shall be receipted to DHSMV when so received and stored in a secure area by the Traffic Unit Supervisor.

    d. The paper citations shall be distributed to each Station Commander or his designee by the Traffic Unit Supervisor and receipted by the same who shall be responsible for their safe storage.

e. The Station Commander or his designee shall enter each citation book into the log book by citation books numbers and later depict to whom the citation book was issued.

f. Members needing a new citation book shall present their depleted citation book with all copies of citations from that book to the Station Commander or his designee for accounting. A check against Smart Cop Mobile Forms shall be performed to ensure that all citations in the book have been correctly issued and entered into the system.

    1) Once all citations are accounted for from that book the Station Commander shall so note it in the original citation issue form for that particular book.

    2) This shall be done prior to issuing a new citation book.

    3) Unaccounted for citations shall be resolved and the resolution noted on the original citation issue form.

g. Once issued to the employee, the member shall examine the citation book ensuring all citations are present. After such, the employee shall sign the cover receipt of the citation book and forward the receipt through the chain-of-command to the Station Commander. The Station Commander shall forward all citation book receipts to the Traffic Unit Supervisor after ensuring entry in the citation log.

h. Should the examination of the citation book show missing citations, the member shall return the book for issuance of another. If the citation is lost or stolen from the member, they will contact the Traffic Unit Supervisor by the respective Station Commander immediately.

i. Books with missing citations shall be returned to the Traffic Unit Supervisor by the respective Station Commander. The Traffic Unit Supervisor shall send the entire book back to the DHSMV with a cover letter depicting he problem. A copy of the letter shall be kept on file with all other citation accountability records.

j. In the case of damaged citations, due to error, only voiding of the citation is necessary. All four copies of the citation shall be marked "VOID". The officers "pink" copy shall be retained by the employee for accounting purposes. Entry is to be made for each voided citation into the Smart Cop Mobile Forms system.

k. Transmittal sheets shall be maintained by each District Records Unit. At the close of each calendar year these transmittal sheets will be forwarded to the Traffic Unit Supervisor for proper maintenance awaiting an audit form DHSMV.

l. Citations that are returned upon a member leaving this agency shall not be issued, instead they shall be marked "VOID", and forwarded to the Traffic Unit Supervisor for submission on transmittal to DHSMV.

m. Defendant shall receive the yellow copy, pink maintained by the issuing officer, white copy shall be forwarded to the Clerk's Office, if an electronic citation is issued, defendant shall be issued the printed “defendant” copy and the “court” copy shall be forwarded to the Clerk Office.

n. Periodic Audit

    1) The Station Commander, Traffic Unit Supervisor for traffic units, shall run a computer report for each issued traffic citation book as listed in the Citation Issue Log Book.

2) Citation books where all the citations are accounted for the Station Commander shall so note in the appropriate space for that book.

3) Missing citations: books where a citation number is missing from the sequential number the Station Commander will verify the citation is still un-issued or have the deputy submit a memorandum explaining the reason the citation is missing

4) The Station Commander shall take appropriate corrective or disciplinary action based on the deputy's response.

o. Submission of un-issued citations upon separation from the Office.

1) Deputies are required to submit to their Station Commander all un-issued traffic citations

2) The Station Commander shall take the necessary steps to re-issue the un-issued citations to another deputy or if not practical, the Station Commander shall "Void" all the remaining un-issued citations and have them entered into the office computer system as "Void".

3) The Citation Issue Log Book will reflect the action taken and appropriate information recorded as necessary.

3. Long form Crash reports: All original long form crash reports shall be completed in Smart Cop Mobile Forms module, and will be forwarded to Tallahassee electronically.

4. Short form Crash reports: All original short form crash reports shall be completed in Smart Cop Mobile Forms module, and will be forwarded to Tallahassee electronically.

W. Recording of Arrest Information

1. Whenever any adult is arrested and brought into any Monroe County Sheriff's Office correctional facility, such individual shall be fingerprinted and photographed. In addition, an arrest report shall be completed.

2. Juvenile arrest: refer to Chapter 43.

3. Whenever a person is arrested who has been previously arrested in Monroe County, the Jail Records Section shall insure that any previous information of old files are updated and that the most current photograph is on file.

4. Whenever a person is arrested and transported to a detention facility The Corrections Division shall fingerprint the individual via the LiveScan system. Once fingerprinting is complete the results are then transmitted to FDLE. If for any reason the system is inoperable a ten-print fingerprint card will be utilized, forwarded to the Identification Section then forwarded to FDLE.]

X. Identification Numbers for Persons Arrested: Each person who has been arrested will have only one identification assigned by SmartCop, although the individual may have been arrested on a number of different occasions and thus have been issued different case and arrest numbers relating to them. Identification numbers are not to be duplicated or skipped.

Y. The Jail Records Section shall attach a copy of the convicted felon form in the subjects MNI (Master Name Index) attachments section for all registered convicted felons in Monroe County in compliance with Chapter 775.13 Florida Statute.

Z. Registration of Sexual Predators and Sexual Offenders: This policy is issued with the express intention of outlining, and specifying the Monroe County Sheriff's Office's response to sexual offender and sexual predator registration as mandated by Florida Statute 775.21, and Florida Statute 943. 0435, wherein the Sheriff is required to publicly identify certain persons as sexual predators and/or sexual offenders and also community notification.

1. Definitions

    a. Sexual Predator: A person so named on record by the Florida Department of Law Enforcement, or by the Judge of any Circuit in the United States.

    b. Sexual Offender: Any person sanctioned by any Court in Florida for an offense outlined in Florida Statute 943.0435 (1)(a), and who has been released on or after October 01, 1997, from such sanction.

    c. Booking facility: The Monroe County Sheriff's Office Correctional Facilities.

    d. Access (as a verb): To approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of, any resources of a computer, computer system, or computer network.

    e. Criminal History Information: Information collected by criminal justice agencies on persons, consisting of identifiable descriptions and notations of arrest, detentions, indictments, information, or other formal criminal charge and the disposition thereof.

    f. Offender Registry Information: Any Information collected regarding the identity, employment location, residential information, and/or criminal history of a sexual offender and/or sexual predator.

2. The Sheriff is required to publicly identify sexual predators, and elects to publicly identify sexual offenders according to law. The following procedures are to be used for those purposes.

    a. Persons required to register are to be directed to the nearest booking facility. Since there are time limits imposed on registration deadlines for affected offenders, registration must be possible 24 hours a day, seven days per week.

    b. Initial Registration consists of the following: Offender Based Tracking Number “OBTS” and fingerprints using the “live scan system.” The offense shall be entered as “Sexual Predator or Offender” as described in FSS 923.01. An online registration form will be completed using the FORTS System.

    c. Re-registration is, for all intents and purposes, a booking without issue of Offender-Based Tracking Number (OBTS) or bond. The offense shall be entered as SEXUAL PREDATOR if the individual is a sexual predator or as SEXUAL OFFENDER. All other fate required for Florida Statute 923.01 shall be collected and an online registration completed. No written instruments need to be filled out, with the exception of a fingerprint card and, upon that card, the offenses as aforementioned.

    d. It is required by law that the registering person be photographed; digital mug shots, therefore, shall be taken of each person at the time he/she registers. It is vitally important that these mug shot photographs be of useful quality, since they will be furnished to the news media and to the Florida Department of Law Enforcement is satisfaction of the requirement.

e. Sexual offenders and sexual predators are required to provide verbatim summaries of their arrests according to specifications in Florida Statute 775.21 and Florida Statute 943.0435. All persons being so registered should be questioned in regard to their criminal histories and any other identities or monikers/nicknames they may have used or are using. Thereafter, a check through NCIC/FCIC must be run.

f. The Jail Commander shall promptly forward the fingerprint card (or digital equivalent) a digital photo mug shot to the Florida Department of Law Enforcement.

g. Sexual Predator/Offender Records as Public Information: The whereabouts and identity of sexual predators and sexual offenders are public record, as is their criminal histories. While FCIC/NCIC computerized criminal history may NOT be distributed, the contents of same as they relate to sexual predators and sexual offenders are public record as specified in Florida Statute 775.21. Furthermore, the Public Information Officer, or any other member of the Sheriff's Office, shall divulge this information on demand. If the victim of any sexual predator or sexual offender was a minor at the time of the offense(s) that fact should be part of the public record, even allowing for the exact age of the victim to be divulged. Under NO circumstances, however, is the identity of ANY victim of ANY sexual offense to be a public record, regardless of the victim's age at the time of the offense.

h. The Major Crimes Unit will be responsible for community notification and compliance. The Major Crimes Unit will notify the Public Information Officer of the registration of a sexual predator, furnishing the computerized criminal history and other criminal justice information to the Public Information Officer for use by the media.

i. The Major Crimes Unit will prepare a flyer on all sexual predators and selected offenders for distribution.

j. Copies of sexual predators and sexual offenders flyers are made available, upon request, by the Major Crimes Unit. These copies shall be provided at no cost to individual citizens or organizations demonstrating a mission that requires contact with children as a focal point of said mission.

k. The flyer shall contain the information regarding the sexual predator/offender and photograph. A short explanation of the public notification law and instructions on where to find further information will also be provided.

l. In addition to the above notification, Florida law requires that within 48 hours after receiving notification of the presence of a sexual predator, the Sheriff of the county where the sexual predator establishes or maintains a permanent or temporary residence shall notify each licensed day care center, elementary school, middle school, and high school within one mile radius of the temporary or permanent residence of the sexual predator or the presence of the sexual predator.

m. The Major Crimes Unit will make these notifications as required. Notification shall be made to a person of authority at each location (Principal, Director, Owner, etc.) If the school is closed for holiday, vacation, etc. in-person notification shall be made upon reopening.

n. The Major Crimes Unit will also, at least quarterly, ensure that contact is made with all identified predators and offenders. Once verification of address is made, entry into FDLE Sexual Predator and Offender databases will be made a written report will be on file.

AA. Criminal History

1. The Sheriff's Office accesses computerized criminal history information through the following computer systems:

    a. Sheriff's Office main frame computer system,
    b. Florida Criminal Information Computer (FCIC),
    c. National Crime Information Computer (NCIC)

2. Only designated terminals in Central Records, Warrants, Communications, and Jail Records (including satellite jail facilities) will be enabled to function as full access F/NCIC terminals.

3. Only persons who have passed the Criminal Justice Information Services certification test will be allowed to access criminal histories from a F/NCIC terminal.

4. User profiles and passwords shall be required to access the mainframe, FCIC/NCIC computer systems.

5. The release of criminal history information from the FCIC/NCIC systems is governed by the Florida Department of Law Enforcement (FDLE) and is only released for law enforcement purposes to authorized personnel.

    a. Dissemination: Receipt of Criminal Histories

        1) Criminal histories can only be disseminated by personnel assigned to Central Records, Warrants, Communications and Jail Records (including satellite jail facilities) and shall only be disseminated to law enforcement personnel (local, state and federal) for law enforcement purposes.

        2) It is recommended that law enforcement officers needing a criminal history obtain it through Central Records or Communications.

        3) If a member of the public requests a criminal history from the Office they should be referred to the Florida Department of Law Enforcement.

    b. Dissemination Log

        1) Authorized personnel disseminating criminal histories shall maintain a log will be kept for all criminal histories disseminated to other authorized criminal justice agencies for a period of four years.

        2) The log shall note the date, name of requesting officer, ID number, if applicable, officer's agency, name of subject person and subject's FBI and /or SID number.

6. Terminal Security

    a. FCIC/NCIC designated terminals shall be accessed with user names and passwords.

    b. When a terminal is to be left unattended for any period of time it should be locked or the user shall log off the system.

    c. The terminal monitor should be positioned where unauthorized people cannot view it.

7. Destruction of FCIC/NCIC Documents

    a. All FCIC/NCIC documents shall be secured by the Office personnel receiving them to prevent access by non-authorized persons.

b. If the documents become part of a case report it shall be included in the submitted paperwork or placed into evidence.

c. If the document has lost its law enforcement usefulness it shall be destroyed and disposed of at a Sheriff's Office facility, preferably by shredding the document.

8. Violation of these rules may result in termination of computer access and discipline or employment termination. Termination of access may occur without notice and is not a disciplinary action.

BB. Computers and Data Network [CALEA 41.3.7]

1. Definitions

a. Sheriff Office Computer: Any computer or digital device (this includes smartphones or tablets) purchased with funds from or administered by the Monroe County Sheriff's Office, regardless of where the computer or device is physically located. This includes computers or devices assigned to members for use at home or in their vehicles. Such computers or devices are usually, but may not, be identified by an inventory sticker.

b. Data Network: Any direct physical medium used to inter-connect the computers of the Monroe County Sheriff's Office. For the purpose of this definition, the term "network" also includes all the equipment and software used to operate, manage and maintain these connections. This is meant as the secure physical Sheriff's Office locations (i.e. headquarters, sub-stations and jails).

c. Remote Access: Any medium that is used to connect to the data network that does not directly connect to the Sheriff's Office. This includes wireless (i.e. WIFI), cellular, dial-up, or any other temporary connections from a location that is not secure.

d. Criminal Justice Information (CJI): Any information that identifies persons that have had contact with the Sheriff's Office. This includes physical characteristics, demographics and any criminal history. This is the information typically stored in the Master Name Index. It also includes information obtained via the F/NCIC system.

e. Digital Device: Any digital computing technology. This includes, but is not limited to, desktop computers, laptop computers, smartphones and tablets.

f. Advanced Authentication: User identity verification that includes a second method of authentication besides user password.

2. The information Systems (IS) group is solely responsible for the confidentiality, integrity and availability of the Sheriff's Office computers, data network and the information stored therein. The duties of IS shall include (but not necessarily be limited to) the following:

a. IS shall ensure that all user passwords meet the following criteria:

1) They shall be a minimum of ten (10) characters.
2) Not be a dictionary word or proper name
3) Not be the same as the user ID
4) Upper and lower case alphabetic characters (i.e. A through Z and a through z) and at least one numerical digit (i.e. 0-9) and at least one special, non-alphabetic character (i.e. ~!@#$%^&*-+=`|\(){}[]:;"'<>,.?/)
5) Not be identical to the previous ten passwords
6) Not be transmitted in clear text
7) Not be displayed when entered

b. IS shall disable any user account that has not been logged onto for more than 90 days.

c. IS shall backup all critical data at least once a day. This data will include all the financial information, CJI, the network shares of the user home directories (including user documents) and user profiles, and email systems. Periodically, IS will restore a subset of backup data to a scratch area to verify that the data can be restored if necessary.

d. All computers will be properly disposed of by Information Systems by authorized methods such as wiping the hard drive or reformatting it.

e. All members of the Information Systems division will have completed, and maintain current certification of, the online CJIS Security Awareness training.

3. Members of the Monroe County Sheriff's Office shall observe the following guidelines: [CALEA 11.4.4, 41.3.7]

a. No member shall allow any other person to use his or her login name and password.

b. No member may connect personal (i.e. owned by the member) computers or digital devices to the Monroe County Sheriff's Office network without the express permission of Information Systems.

c. Only Sheriff’s Office computers may be used to access CJI. Member owned devices may only be used to access email or non CJI.

d. Sheriff’s Office members that access CJI from any remote location must use advanced authentication and must either be CJIS certified or have passed the CIS security training.

e. No member may access CJIS information without a CJIS security certification. These CJIS certifications need to be filed with the training division before security access is granted.

f. Members may use e-mail and internet services. Such services are intended for the member to use in the performance of work duties. Personal use should be limited and not interfere with work duties. Nor shall it be used to access illegal or pornographic material unless in the performance of a members work duties. E-mails shall not be derogatory to fellow members or about any particular social group, based on race, religion, ethnic background or other defining factor.

g. No member may in any way attempt to gain unauthorized entry to computer data, or network of other agencies that the Monroe County Sheriff's Office is connected to. This is also known as browsing.

h. No member may attempt to breach the security of, hack or crack computers, networks and systems of the Monroe County Sheriff's Office and agencies that the Sheriff's Office is connected to. This does not apply to Information System personnel in the performance of their assigned duties.

i. No member may attempt to alter or reconfigure any computer or network without the express written permission of Information Management.

j. The use of software without an approved license agreement is prohibited.

k. No member may install or use any software on the Monroe County Sheriff's Office owned or operated computer system unless approved by the Director of Information Systems Management.

l. No member may bypass or modify any installed security or menu systems without the written permission of the Director of Information Systems Management.

m. No member may install accessory hardware on any MCSO owned or operated computer system unless approved by the Director of Information Management Systems. However, members may use removable memory devices to access or transfer data files only in the performance of their assigned work duties. Removable devices include, but are not limited to, memory sticks, memory cards, floppy and removable external hard drives.

n. Violations of these rules may result in the termination of computer access and discipline or termination of employment. Termination of access may occur without notice and is not a disciplinary action subject to appeal.

4. Reading Agency E-Mails: Each member shall open beyond the preview window and read their e-mails a minimum of one time per shift. Further, when an e-mail has a receipt request tag the member shall not disable a return receipt being returned to the sender for tracking and accounting purposes.

5. Virus Infection Control

   a. As all internet functions are through the network, Information Management is responsible to implement measures to prevent infection of the network by computer viruses, worms, or other program intended to disrupt, seal or cause a failure in the network and hardware.

   b. Every member who has access to any Office owned computer or other device interconnected with the Office network/hardware is responsible to make every effort to prevent infection of the network by computer viruses, worms, or other program intended to disrupt, seal or cause a failure in the network and hardware.

6. Verification of Passwords Security Controls

   a. Every Sheriff's Office network user can only access the network though a user name and password. The password is changeable and the user is encouraged to periodically change the password.

   b. Data modules are further password protected, access limited and read/write/delete options will be determined by position and job requirements.

   c. Information Systems will monitor computer network system activity at a minimum weekly for possible access and improper use violations, as well as attempts by outside sources at system security breaches.

      1) Violations or attempts at security breaches will be addressed immediately.

      2) Internal violations will be reported to the appropriate commander for investigation and possible disciplinary action.

      3) An audit of passwords done continually, but at a minimum bi-monthly, to include removal of former employees from network access.

7. Access Restrictions/Usage

a. Members must be given access privileges to the Office's computer network via Information Management.

b. Specific programs may require specific access based on use certification or necessity due to job function. In these instances only those employees that meet the access criteria shall be given such access. Access can be withdrawn when an employee no longer needs such access, no longer meets certification requirements or has been found to violate access restrictions and use.

c. All programs of a specific criminal justice nature, which provides otherwise non-public record information used in the performance of job duties shall not be used for any personal reasons.

b. Generic programs i.e. Word, PowerPoint, etc. members may access them for personal use as long as it does not interfere with the performance of their work duties.

8. Network Back-up / Electronic Format Records Retention

a. Network/data backup will be accomplished in two ways:

1) Running a redundant server in two or more locations—one or two of which will be physically located at other than the Sheriff's Office headquarters building, Information Systems Management office area.

2) Daily backup tapes will be stored in a secure room at the main corrections facility or removed off site and physically kept by the Assistant Information Management Director.

3) In the event of an anticipated Hurricane landfall, backup media will be shipped outside of Monroe County for safe keeping.

b. Data/Records stored electronically will be retained in compliance with the Florida Records Retention Schedule GS1-L & GS2.

CC. Uniform Crime Reports: The following procedure shall be used for collecting and submitting crime data to the Uniform Crime Reporting program.

1. Records division personnel will review each report to ensure appropriate UCR information has been collected. Applicable reports will be coded for UCR purposes and entered into the UCR statistics computer program in accordance with the Florida Department of Law Enforcement UCR manual.

2. The Records division enters the appropriate code in the UCR program for each reportable offense committed within the county of Monroe. The statistics are generated via computer, and all required crime information is reported to the Florida Department of Law Enforcement. UCR information is reported semi-annually and annually, according to their established guidelines and by their established deadlines.

3. The Florida Department of Law Enforcement then forwards the appropriate information to the National system for Uniform Crime Reporting.