

**CHAPTER FIFTY-TWO**  
**INFORMATION MANAGEMENT / RECORDS**

**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 SmartCop System and Records Section.

**II. DISCUSSION**

It is the policy of the Sheriff that the Office have 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 Section, is supervised by the Records Supervisor, who is directly responsible to the Director of Court Services/Central Records.

A. The main function of the Records Section are 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 latter 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 which is legal to release and protecting any confidential information from inappropriate, untimely, or illegal release. The following information 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. Information revealing undercover personnel of any criminal justice agency.
4. Criminal intelligence or criminal investigative information which could reveal the identity of the victim of a sexual battery as defined by Florida law.
5. Information revealing surveillance techniques, procedures, or undercover personnel.
6. Criminal intelligence or information which reveals the personal assets of the victim of a crime, other than property stolen or destroyed during the commission of a crime.
7. Criminal intelligence and investigative information received by a criminal justice agency prior to January 1979.
8. The home address, telephone numbers, and photographs of law enforcement personnel; the home addresses, telephone numbers, photographs, and places of employment of the spouses and children of law enforcement personnel; and the names and locations of schools attended by the children of law enforcement personnel.
9. 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.
10. 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.

B. Responding to requests for information in Police Reports

1. When a member of the public request information or access to police reports from any member of the Sheriff's Office, that person is to be directed to the Records Division in each respective sector with the exception of the Cudjoe Sub-Station, which is responsible for releasing to the public or making available for public review any information from any police report in any form.
2. In order to serve the public in a more timely manner, any request from the public to review the daily reports that are not case specific and have been processed by the Sector Records Section, shall be referred to the Public Information Office in the Community Relations Division, which is responsible for releasing any information from any police report. This paragraph does not preclude, however, the Records Division giving every effort to the releasing of such requested records to the public
3. 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 Court Services/Central Records.

C. Direct Access

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

1. Only personnel assigned to the Records Section shall have direct access to Record Section files. All other personnel of the Sheriff's Office shall be able to access records through the SmartCop system without the help or permission of the Records Section. Access to these records is assigned by the Director or Court Services/Central Records and is dependent on the employees job function.

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

D. Duplication of Office Records

1. Office records may only be duplicated for official purposes.
2. Official Sheriff's Office records shall not be used in conjunction with educational study projects, surveys, academic research, unless approved by the Sheriff.
3. Official records or duplications thereof shall not be retained in personnel files or maintained outside of the Office.

E. Juvenile Records

1. Electronic juvenile records shall be tagged as a 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 985.11 Florida Statute, 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 39.12 (2) Florida Statute.

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 imitate the following procedural steps to insure that the requirements of law are met. ALL COURT ORDERS MUST BE CERTIFIED
  - a. All court orders must be accompanied by a certificate of edibility from the Florida Department of Law Enforcement.
  - b. Any criminal history where a defendant was found or plead guilty, of the following offenses, without regard to whether adjudication was withheld.

1) Florida Statute 794	Sexual Battery
2) Florida Statute 800.04	Lewdness / Indecent Exposure involving a child
3) Florida Statute 817.034	Florida Communication Fraud Act
4) Florida Statute 827.071	Child Abuse / Sexual Performance by a child
5) Florida Statute 839	Offenses by Public Official / Employee
6) Florida Statute 907.041	Pretrial Detention and Release
2. Any request for a criminal history 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 to:
    - Florida Department of Law Enforcement
    - Crime Information Bureau - records Control Unit
    - Post Office Box 1489
    - Tallahassee, Florida 32303
  - d. Include in the mailing a copy of the motion and affidavit if obtainable.
  - e. Notify all agencies to which the subjects affected records has been disseminated.
4. Administrative or juvenile
- a. Identify the subject of the court order or document requesting expungement or correction 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:
    - Florida Department of Law Enforcement
    - Crime Information Bureau - Records Control Unit
    - Post Office Box 1489
    - Tallahassee, Florida 32303
  - d. Notify all Office divisions to which the subject's affected record has been disseminated.
5. All expunged / sealed records shall be held in pending status until a reply letter has been received from the Florida Department of Law Enforcement. Upon receipt of the reply letter, complete the expunge / seal or any other action cited in the Court Order or document requesting expungement or correction.
6. Scanning Expungments
- a. Once a legal letter has been received from the Florida Department of Law Enforcement stating a record was expunged, Central Records will do the following:
    - 1) Collect all records pertaining to the file
    - 2) Destroy all documents with the exception of the F.D.L.E. letter & Court Order
    - 3) Scan the F.D.L.E. letter
7. Scanning Sealed Records
- a. Once a legal letter has been received from the Florida Department of Law Enforcement, stating a record has been sealed; Central Records will do the following:
    - 1) Collect all records pertaining to the file.
    - 2) Scan all documents along with F.D.L.E. letter and court order.
    - 3) Verify all paperwork ahs been scanned and is legible, then destroy.
8. Scanning Records with Special Circumstances
- If there several suspects listed, but only one person's records are being sealed or expunged Central Records will do the following:
- a. Sealed Records:

- 1) Once a legal letter has been received from the Florida Department of Law Enforcement, stating a record has been sealed; Central Records will do the following:
  - a) Collect all records pertaining to the file
  - b) Redact all required information
  - c) Re-scan; replace the paperwork already scanned, as well as the letter from F.D.L.E.
  - d) Destroy all paperwork

b. Expunged Records

- 1) Once a legal letter has been received from the Florida Department of Law Enforcement, stating a record has been expunged; Central Records will do the following:
  - a) Collect all records pertaining to the file
  - b) Redact all required information
  - c) Re-scan; replace the paperwork already scanned, as well as the letter from F.D.L.E. and court order
  - d) Destroy all paperwork

9. The file within the 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 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 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) Insure 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 such report 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 affix his/her initials and ID number in the lower right margin of the report.
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 employee. It is the employees 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 employee's supervisor, who rejects an incident report shall:
    - 1) E-mail the employees supervisor that the report has been rejected. The employee's supervisor will then forward to the originating employee.
    - 2) Employees shall follow previously outlined procedures for correcting and returning the report.
  - c. Uniform Crime Report (UCR) classification personnel who believe an incident report would be rejected shall forward the report to the appropriate Sector Commander for review and appropriate action.
4. Routine Reports - Once the supervisor has reviewed the reports, the Sector Records Unit will distribute to the appropriate agencies and forward to Central Records. copies of reports may be maintained at the Sector Stations in an appropriate filing system.
5. Routing Reports
- a. Law enforcement supervisors are authorized to review, approve, route and or refer reports.
  - b. Supervisor will also make copies of any support documents and route the documents to the referred unit.
  - c. Original support documents will be sent to the Records Unit, 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 Disposition field.
    - 1) Cleared by arrest
    - 2) Exceptionally cleared
    - 3) Unfounded
    - 4) Active

5) Inactive

J. Report Distribution

1. Investigative reports - will be distributed by the reviewing patrol supervisor or investigative supervisor. Most reports are in electronic format and may distributed as such.
2. Supplemental reports - same procedures will be followed as with initial reports.
3. Insurance reports - 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 Community Relations 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.**  
Revised 08/26/09
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 assed according to the established schedule.

K. 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 reports are forwarded to Central Records for master control and filing.
- c. Whenever incident reports are received in Central Records, incident numbers are matched to the appropriate report utilizing the C.A.D. report. The Central Records Administrator 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 placement with the original report. The Sector Records Unit shall maintain all follow-up reports and forward them to Central Records every ten (10) days.

L. Daily Audit

An audit shall be conducted by the Central Records section of all case numbers drawn each day. This is to insure that all reports and follow up reports are received and accounted for.

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 Court Services/Records Management, shall be allowed beyond the point so designated.

N. Records Retention Schedule

All records are retained according to the GS1-L 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.

**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 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. An modus operandi file

R. The Corrections Record Section shall maintain:

1. A booking file on each person arrested to include;
  - a. Updated information obtained from State and Federal rap sheets (i.e. FDLE, FBI and fingerprint classification number)
  - b. Photograph
  - c. 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 and Wanted Persons Files

1. All warrants directed to be served by the Sheriff of Monroe County, Florida, shall be logged by the Warrants Section in to the Master "Warrants Log", which may computerized.
2. FCIC / NCIC Entry
  - a. All such warrants shall then be entered into the state FCIC (Florida Crime Information Center) and national NCIC (National Crime Information Center) computers.
  - b. Felonies - In the remarks 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 stating otherwise.
  - c. Misdemeanors - In the remarks section it will be noted "Florida Pick-up Only", unless there is a warrant information sheet from the State Attorney's Office stating otherwise.
  - d. Warrant's personnel entering information are both FCIC and NCIC certified.
  - e. Juvenile orders to take into custody are entered in F/NCIC computers.

3. Once logged and processed, the original warrant is filed in the current filing area.
4. Out-of-State Warrants - After extradition is confirmed, all information is forwarded to the Extradition Coordinator to take care of the following:
  - a. Forward a certified copy of our original warrant to the Sheriff of the County in the State of jurisdiction along with a letter, certified copy of the affidavit and/or information
5. Should a warrant be received from another jurisdiction, the warrant is forwarded to the appropriate Sectors for service. If unable to be served, the warrant is returned to the Warrant Section, where a cover letter is prepared and attached to the warrant, which is sent back to the originating jurisdiction.
6. Warrants shall be cancelled for service and recall only - Should a warrant be canceled, notice shall be given to all personnel involved.
7. Prior to service of any warrant, verification will be made.
  - 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 telephone or teletype.

#### V. Traffic Citation Records

1. Records retention of citations
  - a. All citations and warnings shall be entered into the SmartCOP system under section U.C.M.
  - b. All citations and transmittal slips shall be forwarded to the Clerk's Office, by each appropriate Sector, within five (5) days after being written.
  - c. Copies of citations may be kept by Sector Records Unit.
  - d. It shall be the duty of each respective Sector Commander to ensure the entry of the Citations and Warning into the SAMRT COP system and the transmittals to the Clerk's Office are accomplished in the specified time.
  - e. It shall be the duty of Sector Records Unit, under the direction of the Sector Commander to audit the information, sending back requested changes, to the originating Deputy.
2. Citation Accounting
  - a. Citations are ordered from the DHSMV, Tallahassee, by the Traffic Unit Supervisor on an as need basis.
  - b. Sector Commanders shall advise the Traffic Unit Supervisor of their need for citations.
  - c. Citations shall be receipted to DHSMV when so received and stored in a secure area by the Traffic Unit Supervisor.
  - d. The 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.
  - 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 employee shall return the book for issuance of another. If the citation is lost or stolen from the employee, they will contact the Traffic Unit Supervisor by the respective Station Commander immediately.
  - [34.08M d]
    - 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 the problem. A copy of the letter shall be kept on file with all other citation accountability records.
    - [34.08M d]
      - j. In the case of damaged citations, due to error, only voiding of the citation is necessary. All five copies of the citation shall be marked "VOID". The fifth or officers "pink" copy shall be retained by the employee for accounting purposes. Entry is to be made for each voided citation into the SmartCOP system under U.C.M.
    - [34.08M e]
      - k. Transmittal sheets shall be maintained by each Sector 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 an employee 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, while the blue copy is maintained by the Traffic Unit.
  - n. Periodic Audit of Citations - refer to Chapter 40 - traffic, page 16 for requirements and procedures for an annual audit of all issued traffic citations.
    - [34.08M e]

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. [CALEA 1.2.5 a,b]
- 2. Juvenile arrest - refer to Chapter 43.
- 3. Whenever a person is arrested who has been previously arrested in Monroe County, the Corrections Records Section shall insure that any previous addresses of old files are updated and that they most current photograph is on file.
- 4. The Identification Section shall verify the identities of persons arrested in Monroe County. The Corrections Division shall send two ten-print fingerprint cards or electronic version thereof, one care

for other agencies on all Monroe County Sheriff's Office arrest to the Identification Section within one working day after a person has been arrested. The Corrections Division will use cards provided by FDLE, the OCA number will be the same number as on the mug shot. Once fingerprint cards are received, they will be checked for completeness and the quality of the fingerprints. Once card will be classified according to the Henry System. A local name check and fingerprint file search will be completed. One card will be sent to FDLE Crime Information Bureau. The second card shall be returned to the Corrections Division. Once an individual has been released from the Corrections Division, the Corrections copy of the fingerprint shall be forwarded to the Identification Section or inclusion into the Master Fingerprint File. Only the best fingerprint card will be maintained in the Master System. [CALEA 1.2.5 b]

X. Identification Numbers for Persons Arrested

Each person who has been arrested will have only one identification, although the individual may have been arrested on a number of different occasions and thus have been different case and arrest numbers relating to them. Identification numbers are not to be duplicated or skipped.

Y. The Corrections Records Section shall maintain a file of 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 was 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 person 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. Person 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. 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" if the individual is a sexual offender. All other fate required for Florida Statute 923.01 shall be collected and a Physical Descriptor Report shall act as repository of same. No written instruments need to be filled out, with the exception of a fingerprint card and, upon that card, the offenses as aforementioned.
- c. 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.
  - d. 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, with paper copy of the responses and all pertinent queries forwarded to the Director of Central Records along with the fingerprint card.
  - e. The Director of Court Service/Records Management shall:
    - 1) Promptly forward the fingerprint card (or digital equivalent) an digital photo mugshot to the Florida Department of Law Enforcement, and
    - 2) Notify the Public Information Officer of the registration, furnishing the computerized criminal history and other criminal justice information to the Public Information Officer for use by the media.
    - 3) Notify the Intelligence Officer of the registration and furnishing the computerized criminal history and other criminal justice information to the Intelligence Officer for use by law enforcement. The Intelligence Officer will furnish the Sergeant of CAWACU with all the information pertaining to the sexual predators and sexual offenders.
  - f. Sexual Predator / Offender Records as Public Information - The whereabouts and identity of sexual predators and sexual offenders is 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 is a public record as specified in Florida Statute 775.21. Furthermore, the Public Information Officer, or nay other employee 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.
  - g. The Crime Against Women and Children Unit (CAWACU) will be responsible for community notification and compliance.
  - h. CAWACU will prepare a flyer on all sexual predators and selected offenders for distribution.
  - i. Copies of sexual predators and sexual offenders flyers are made available, upon request, by CAWACU. 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.
  - j. 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.
  - k. 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.

- I. CAWACU 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.
- m. CAWACU 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 system:
  - 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 FCIC terminals.
3. Only persons who have received FCIC authorization will be allowed to access criminal histories from these terminals.
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 FCIC/NCIC and is only released for law enforcement purposes.
  - 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 officers (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 request 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 include Office personnel.
    - 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 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 person 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.

#### AB. Computers and Data Network

1. Definitions
- a. Sheriff Office Computer - Any computer purchased with funds from or administered by the Monroe County Sheriff's Office, regardless of where the computer is physically located. This includes computers assigned to members for use at home or in their vehicles. Such computers are usually, but may not, be identified by an inventory sticker.
  - b. Data Network - Any medium used to inter-connect the computers of the Monroe County Sheriff's Office. This includes wireless, dial-up and other temporary connections. For the purpose of this definition, the term "network" also includes all the equipment and software used to operate, manage and maintain these connections.
2. Employees of the Monroe County Sheriff's Office shall observe the following guidelines:
- a. Users of the network should log off the network when they have completed their work (i.e. the end of the day) to conserve on this resource.
  - b. No employee should allow any other person to use his or her login name and password.
  - c. No employee may connect personal (i.e. owned by the employee) computers to the Monroe County Sheriff's Office network without the express permission of Information Systems.
  - c. **Employees may use e-mail and internet services. Such services are intended for the employee 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. E-mails shall not be derogatory to fellow employees or about any particular social group, based on race, religion, ethnic background or other defining factor.**  
(Effective 6-11-2008)
  - e. No employee may download or otherwise copy any material from the Internet or any other computer that is illegal or pornographic in nature, other than in the course of a criminal investigation.
  - f. No employee may use the Monroe County Sheriff's Office computer or network to produce or distributing any material that is illegal or pornographic.

- g. No employee may in any way attempt to gain unauthorized entry to computer data, or network of other agencies that the Monroe County Sheriff's Office us connected to. This is also known as browsing.
- h. No employee 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 employee may attempt to alter or reconfigure any computer or network without the express 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 employee may bypass or modify any installed security or menu systems without the expressed 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.

### 3. Reading Agency E-Mails

Each employee 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 employee shall not disable a return receipt being returned to the sender for tracking and accounting purposes.

**Revised 01/19/10**

### 4. 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 employee 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**

(Effective 6-11-2008)

### 5. 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.

**6. Access Restrictions / Usage**

- a. **Employees 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.**
- d. **Generic programs i.e. WORD, PowerPoint, etc... employees may access them for personal use as long as it does not interfere with the performance of their work duties.**  
(Effective 6-11-2008)

**7. Network Back-up / Electronic Format Records Retention**

- a. Network/data back up 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 back-up 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 to HIDTA San Diego for safe keeping.
- b. Data/Records stored electronically will be retained in compliance with the Florida Records Retention Schedule GS1-L & GS2.

(Entire Chapter Revised 11/30/2007)