SOUTH MIAMI
POLICE DEPARTMENT

GENERAL ORDER NUMBER: 34.1	DATE OF ISSUE: July 31, 2011	EFFECTIVE DATE: March 30, 2018	NUMBER OF PAGES: 09
CFA STANDARD: 26, 32 SUBJECT: Records - ADMINISTRATION	NEW (X) RESCINDS (X) AMENDS ( ) OTHER ( )	By Order Of: Rene Landa, CHIEF OF POLICE	

CFA STANDARDS: 26.01M, 26.02M, 26.03M, 26.04M, 26.05, 26.06M, 26.07M, 26.08, 26.09M , 32.01

SECTIONS:

34.1.1	**Privacy and Security**
34.1.2	**Records Retention Schedule**
34.1.3	**Uniform Crime Reporting Program (UCR)**
34.1.4	**Operational Accessibility**
34.1.5	**Report Accounting System**
34.1.6	**Computer System Passwords**
34.1.7	**Software & Computer Disks**
34.1.8	**Computer System Back-up**
34.1.9	**Computerized Criminal Histories**
34.1.10	**Computer Usage**

RESCINDS: All existing orders in conflict.

PURPOSE: To provide guidelines for Records functions; to provide procedures for submitting, reviewing and controlling departmental reports; to ensure that proper record security and controlled record distribution is maintained; to establish procedures for police department records retention. Electronic records governed by FBI CSP rules, including FCIC and NCIC, will to a minimum adhere to the FBI CJIS Security Policy (FBI CSP).

SCOPE: All departmental personnel.

POLICY: It is the policy of the South Miami Police Department to meet the managerial, operational, and informational needs of the department and the public by maintaining an accurate and easily accessible records system in compliance with FSS 119.

PROCEDURE:

34.1.1 Privacy and Security

Access to the Records Section during business hours is restricted to Records Function personnel, the Chief of Police, Assistant Chief, Division Lieutenants, and the Accreditation Manager. Other persons needing information will contact Records Section personnel for assistance. Only those with legitimate access to review files or restricted computer monitors will be allowed into the Records Section. [CFA26.03]

A. The Records Function maintains separate hard copy files for all juvenile and adult criminal records for those reports that exist in that form. Computer generated reports are flagged as Juvenile Confidential by the Report Management System and Records Unit and personnel shall review their entry for proper entry.

B. In accordance with Florida State Statute Chapter 39, "Any law enforcement agency may fingerprint and photograph a child taken into custody upon probable cause that such child has committed a violation of law." The fingerprinting and photographing of juveniles taken into custody is a function that the Department defers to the Miami-Dade Juvenile Assessment Center (JAC). .

1. Juvenile arrest reports, fingerprint records (if applicable), photographs and other forms of identification, or copies thereof, are marked as being confidential, unless authorized to be released by Florida law. [CFA26.07M]

2. Juvenile arrest reports, criminal history files, fingerprints and photographs (if applicable) will be kept separate from adult criminal history files, fingerprints and photographs. [CFA26.08]

3. <u>Expunging And Purging Juvenile Records</u>: When a certified order for sealing or expunging a record is received from the Clerk of the Court, the Records Clerk will comply with the following procedures:

   a. Record the date and time received on the back of the order;
   b. Check the name in the computer and pull the file;
   c. Determine if the order directs a partial or complete sealing or expunging;
      (1) The court may only order sealing/expunging a criminal history record pertaining to one arrest or only a portion thereof, or one incident of alleged criminal activity; or
      (2) The court may, at its sole discretion, order the sealing/expunging of a criminal history record pertaining to more than one arrest if the additional arrests directly relate to the original arrest;

(3) If the court intends to order the sealing/expunging of records pertaining to additional arrests, such intent must be specified in the order.

d. The letter requesting sealing/expunging, a certified copy of the court order, and the FDLE certificate of eligibility, along with the entire case file, will be placed in the locked Sealed or Expunged file;

e. All arrest data will be deleted;

f. The original letter from FDLE requesting the seal/expunge action will be placed with the case file. On expungement orders, the arrest reports will be destroyed and a copy of the order will be filed.

4. Juvenile records, with the exception of capital offenses, may be destroyed if they meet the retention guidelines set by Florida State Statute. [CFA26.08]

5. Access to records of juvenile offenders is limited. However, the subject of juvenile offense records may authorize access to such records to others (such as a potential employer) by means of a signed release if they have reached majority age, otherwise only through a release signed by their parent or legal guardian. [CFA26.08]

6. Confidential photographs of juveniles taken into custody pursuant to Florida State Statutes: "may be shown by a law enforcement officer to any victim or witness of a crime for the purpose of identifying the person who committed such crime."

7. Unless otherwise ordered by the court, if the child is found to have committed an offense which would be a felony if committed by an adult, then the law enforcement agency having custody of the fingerprint and photograph records (i.e. the JAC) will retain the originals and immediately thereafter forward adequate duplicate copies to the court, with a written offense report and/or arrest affidavit relating to the matter for which the child was taken into custody.

8. Law enforcement officers and Records Function personnel will have access to juvenile criminal history files, fingerprints and photographs on an as needed basis. All law enforcement agencies and the Florida Department of Law Enforcement (FDLE) will use these fingerprint and photograph records only for identification purposes. If identification is made, FDLE will advise the law enforcement agency of this fact and the name and last known address of the child.

C. Information contained in written reports stored in the Records Section will be released in accordance with the guidelines established in FSS 119.07, General Order 27.1, and General Order Chapter 34 (Records).

34.1.2 Records Retention Schedule

It shall be the policy of the South Miami Police Department to ensure that records are retained in accordance with the general records schedule for law enforcement agencies established by the Florida Department of State, Division of Library and Information Services, Records Management Program. A copy of the records retention schedule will be maintained in the records section and it is included in this procedure. [CFA26.01M(b)]

A. Records that have met the retention requirements will be disposed of in accordance with the Florida Department of State, Division of Library and Information Services, Records Management Program. Purging of those files will be done under the supervision of the CID Lieutenant.

State of Florida Retention Schedule:

1. Transitory and personal messages that do not support business purposes should be deleted in a timely manner.

2. Convenience or Reference copies should be deleted from the e-mail system after the record (master) copy has been filed appropriately. "Retain until obsolete, superseded or administrative value is lost."

3. Record (master) copies of public records communicated through e-mail systems like other records have retention values established in accordance with the operational needs of the program function to which they relate and any additional legal, fiscal, or historical value. Generally, records transmitted through e-mail systems will have the same retention periods as records in other formats that are related to the same program function or activity. Where retention schedules already exist agencies should regulate the retention of e-mail records in to those filing and recordkeeping systems.

D. The following records do not meet the retention requirements because they are classified as historical records and are to be retained indefinitely (Capital Crimes):
   1. Abduction/kidnapping
   2. Arson
   3. Child Abuse
   4. Home Invasion
   5. Homicide/Murder
   6. Armed Robbery
   7. Extortion

8. Sexual Battery
9. Bomb Threat

34.1.3 Uniform Crime Reporting (UCR) Program

A. The Records Section is responsible for ensuring that all reports receive the proper coding according to UCR guidelines.

B. Information collected into the computer system will be available for the generation of the UCR codes.

C. UCR statistics are compiled semi-annually and annually by Records personnel. The statistics are reviewed by the Chief of Police and then submitted to FDLE.

D. The report format will be in accordance with FDLE requirements.

34.1.4 Operational Accessibility

A. Records Section personnel will control the accessibility of all reports, records and other information stored in the Records Section. During business hours, Records Section personnel will access and furnish information to agency personnel. The requests for copies of police reports by the public or agencies outside of the Department shall be made during regular business hours, on Monday through Friday between 0800 to 1600 hours, excluding official holidays. [CFA26.02(b)] If a request is made on days or times not specified in this section, the request(s) shall be approved on the next business day following that day the request was received. [CFA26.01M(c)]

B. Records information is accessible to agency personnel on a 24-hour/7 day basis, either through the on-duty Communications/Records personnel or through the Department's computer system and issued password(s). [CFA26.05)] Records information that has been reviewed and entered by the Records Section may be accessed from the central computer network located in the police station. [CFA26.02(a)]

C. Records released to the public will contain only that content that can be released under Florida law. Confidential material (such as the names of juveniles, sexual battery victims, personal information deemed exempt by law involving police personnel, etc.) will be redacted in order to be compliant with Florida law. The records custodian or designee must review the records for compliance prior to release. [CFA26.02M(c)]

34.1.5 Report Accounting System

The Records Unit serves as the central repository for all police reports and other records as determined by the Chief of Police, and is responsible for report accountability, records

maintenance, and records retrieval. It is the policy of the South Miami Police Department to comply ith all federal, state, and local laws in reference to records security, maintenance, retention, destruction, and distribution. The Report Control System is as follows: [CFA26.01M(a)]

A. **All reports will be turned in or transmitted by the reporting officer by the end of his/her tour of duty**. Once the officer's supervisor has approved and signed off on the report [physically or electronically], it will be placed in the approved reports basket located in the police station.

1. If a report is incomplete, the officer will advise his/her supervisor why it is incomplete.

2. The supervisor will advise the officer as to an acceptable date for turning in the completed report.

3. All reports must be turned in before the Officer leaves for the day, so that the CID Division may be apprised of certain serious crimes, such as burglary, aggravated battery, or robberies. Any exceptions to this shall be made only at the discretion of the shift commander.

4. Any supplemental reports will be turned in accordance with the regulations set forth in this General Order.

B. In cases involving reports that fit UCR guidelines the following will occur:

1. As stated in 19.1.3(A), the CID Lieutenant will review all forwarded copies of Offense and Incident Reports on a daily basis (Monday - Friday).

2. All original reports will be forwarded to Records.

C. All original reports will be maintained by Records and filed according to the report's case number.

D. Any time during the process listed in this General Order that a mistake is found with a report, said mistake will be brought to the attention of the reporting officer and, if necessary, his/her supervisor for correction.

34.1.6 Records and Computer System Passwords

The Information Technology Administrator is the System Administrator for the Department's computer system. As such, he is tasked with the issuing of all passwords and access codes to the South Miami Police Department computer network and Records database.

A. Access to various segments of the Department's computer system shall be controlled by passwords and security access levels. The System Administrator shall maintain an inventory of the different users assigned to the Department computer system and Records database.[CFA32.01(e)] Employees will take every available precaution to not divulge their password to any other individuals. This method of security will help safeguard against unauthorized attempts to access, alter, remove, disclose or destroy stored information. [CFA 26.04M(a)] [CFA32.01(d)]

B. There will be annual review of these procedures by the Communications Supervisor to insure that only authorized personnel have access to the computerized files. Personnel who are no longer authorized to have access to such files must be removed from the system within seven calendar days.[CFA 26.04M(c)]

34.1.7 Software & Computer Disks

A. The introduction of outside software and disks could result in the introduction of a virus into the Department's computer system. Therefore, any suspect software or computer disks received from or brought in from outside the department shall be forwarded to the System Administrator. The System Administrator will be responsible for conducting any virus and/or compatibility checks. [CFA32.01(c)]

B. Only software licensed for use in departmental computers, both networked and stand-alone shall be used. Personnel are not allowed to introduce any software into Department owned computers without the approval of the System Administrator.[CFA32.01(c)]

34.1.8 Computer files maintenance, backup, and retention [CFA26.04M(b)]

A. All records and data inputted into the Department's network are backed-up on a daily basis. The System Administrator shall change the back-up tape as required and archive the tapes. Back-up tapes shall be stored in a locked, fireproof media safe. If a back-up tape must be disposed of, it shall be demagnetized prior to disposal to prevent unauthorized records retrieval.

B. Computer users that have information stored on their hard drives are strongly encouraged to back-up their information on a routine basis, since this information is not backed-up unless placed on the network. If not backed-up by the user, this data may be lost forever if there is a catastrophic failure.

C. Maintenance of the electronic files will be done only by personnel approved by the Department. Retention of the files will be done in compliance with Florida state laws dealing with records retention.

D. Destruction of electronic media will be handled in accordance with the FBI CJIS Security Policy, wherein, it states: the agency shall sanitize, that is, overwrite at least three times or degauss (erase) digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (crushed, cut up, shredded, etc). The agency will maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

34.1.9 Computerized Criminal Histories

A. Members of the South Miami Police Department have access to computerized criminal history record information, via the Department's FCIC/NCIC computer system, for criminal justice purposes only. In order for personnel to have access and receive FCIC/NCIC criminal history information, an issued password must be utilized. Each access and request for information is logged by the FCIC/NCIC computer system. Additionally, only those personnel who are FCIC/NCIC certified may access the Department's FCIC/NCIC computer network. The user must renew every two years.

B. Criminal histories are specifically limited for law enforcement use only

C. Access and release of all criminal history records information will be in accordance with the ***Criminal Justice User Agreement*** as established between the South Miami Police Department and the Florida Department of Law Enforcement.

D. Communications personnel will shred and destroy all printed FCIC/NCIC criminal history documentation at each shift change. Departmental personnel are also required to shred FCIC/NCIC criminal history material after the use of such information is no longer needed. Records Function personnel will file all related criminal history information in the appropriate case files. This information will <u>not</u> be released from the Records Function to the public.

E. Personally Identifiable Information is information which can be used to distinguish or trace an individual's identity (such as name, social security number, or biometric records), alone or when combined with other personal or identifying information which is linked or linkable to a specific individual (such as date of birth, place of birth, or mother's maiden name). Any FBI CJIS provided data maintained by an agency may include PII. PII may be extracted from CJI for the purpose of official business only.

34.1.10 Computer Usage [CFA32.01 (a and b)]

The use of departmentally owned computers, laptops, city e-mail, and access to the internet through any of these systems are limited to departmental use only. Officers will only access law enforcement data bases for official law enforcement

reasons. Employees do not have any expectation of privacy as to their use of City provided technology and equipment. All use of the internet, computer network, or other information sharing technology must be conducted in a responsible, efficient, ethical, and legal manner. The employee bears the responsibility to inquire as to acceptable and unacceptable uses prior to such use.