	SFASU POLICE DEPARTMENT	
	Policy 5.1 Departmental Records	
	Effective Date: 04/08/19	**Updated: 04/30/2021**
	Approved: John Fields, Jr. Chief of Police	
	Reference: TBP 5.01, 5.02 5.03, 10.02f / IACLEA 16.1.1a – e, 16.1.2a – e, 16.1.3, 16.1.4, 16.1.5, 16.1.6, 16.1.7, 16.1.9, 16.1.10a - d, 16.2.1a – e, 16.2.2, 16.2.3, and 16.3.1	

I. POLICY

A "records unit" that functions well is critical for the effective delivery of law enforcement services. An efficient means of storing, cataloging, and retrieving records is essential for meeting the management, operational, and informational needs of the police agency.

II. PURPOSE

The purpose of this policy is to assist records personnel in setting up and maintaining an effective record keeping system.

III. RECORDS SECURITY – PHYSICAL FILES (TBP 5.01)

A. The police records unit is housed in restricted areas. Personnel assigned to the records unit (Administrative Specialist Erika Colegio) are directly supervised by the records supervisor (Administrative Specialist to Chief of Police Karen Moore) who reports directly to the Chief of Police.

B. The records supervisor is responsible for maintenance of department records and will be provided training in Law Enforcement Records Management and the Public Information Act.

C. The department maintains information for most records. For the paper records that are kept by the department, they must be stored and secured in the authorized file cabinets located in the administrative specialist's office. All electronic records are maintained on secured servers and housed in a protected area (IACLEA 16.1.11a & b).

D. Access to and retrieval of police records is restricted to assigned records personnel only. Entry by unauthorized personnel is prohibited (IACLEA 16.1.11c).

E. The records unit will be secured and locked when it is not staffed by assigned records personnel.

F. Personnel authorized by the records supervisor or the Chief of Police may have access to the records unit after hours for need-to-know information only. Authorization may be granted to shift supervisors and shift commanders only.

G. When entry has been made by authorized personnel, written notification to the records supervisor will be made within 24 hours of the entry. Written notification must state the date entry was made, time entry was made, why entry was made, and what records were accessed and by whom (IACLEA 16.1.11c).

H. Data maintained on the department's servers will be "backed up" on a continuous basis and all recovery activities shall be performed by a CJIS authorized university Information Technology personnel.

I. Electronic retrieval of all data is password protected and based on an individual's level of access approved by the Chief of Police.

IV. SECURITY OF CENTRAL RECORDS COMPUTER

A. The Universities Instructional Security Officer [ISO] is the administrator for all policies dealing with Stephen F Austin State University and its individual departments. Consistent with University Polices, the SFASU Police Department also embraces the addition of the FBI CJIS Security Policy [CSP] which is administered by the Terminal Agency Coordinator [TAC] (IACLEA 16.1.10a).

B. System Updates: All components of the IT systems with CJIS connectivity shall be updated with all available Security Hot fixes, Updates and Patches within 30 days of availability. The updates are performed by the ISO or his/her designee. This applies to workstations, servers, laptops, switches, routers and all other managed IT equipment.

C. Access: In addition to SFA Policy 14.1.1 Account Management and Control, a user/operator list will be maintained, by the Terminal Agency Coordinator [TAC], that includes the personnel agency-issued credentials of all personnel with unescorted access into physically secure areas of the department. This list will be reviewed annually and as needed; it will be documented when changes are performed. Changes to authorized user accounts may include creating, activating,

modifying, disabling, and removing accounts of authorized personnel and will be reported to the agency administrator (IACLEA 16.1.10c).

Password settings are upper case, lower case, special characters, and expire within 90 days, are not reused for ten iterations and are at least eight characters long. Passwords are not kept in any form and are the responsibility of the user, however the administrator has rights to reset a password in the event the user forgets theirs. The password created by the administrator will be set to temporary and the user will be required to create a new unique password. Each person authorized to access Terminal/MDT data shall receive security awareness training within in six months of appointment or employment and thereafter at least every two years, in accordance with CJIS policy; this training will be documented (IACLEA 16.1.10 d).

D. Backup and Recovery: In addition to SFA ITS Policy 14.1.8, the ISO or designee will conduct backups and or recovery of user-level information contained in the information system within the organization-defined frequency consistent with recovery time and recovery point objectives (IACLEA 16.1.10b).

V. RECORDING OF INCIDENTS BY CATEGORY

A. In order to develop a comprehensive reporting system, it is necessary to record actions taken by law enforcement personnel whether in response to a request for service or for self-initiated actions. Each reported incident occurring within the department's service area will be categorized as one of the following and will receive a unique sequential incident or call for service number:

1. Individual's request for service or assistance to individuals on campus property (IACLEA 16.1.2b).

2. Crime reports, violations of institutional policy or complaints that require one of the following:
   a. an officer to be dispatched;
   b. an assigned employee to investigate; and
   c. an assigned employee to act at a later time.

3. Self-initiated criminal and non-criminal cases by officers (IACLEA 16.1.2c).

4. Incidents involving arrests, citations (other than traffic), or summonses (IACLEA 16.1.2e).

5. Incidences involving outside agencies performing official duties on campus property that request assistance (IACLEA 16.1.1a and 16.1.2d).

6. Personnel have the ability to classify and recall incident records by case number, call for service number, traffic stop number, type of incident and location (IACLEA 16.1.6).

7. The agency will maintain an arrest history of all persons who have been summoned, cited or subjected to a custodial arrest (IACLEA 16.1.9).

B. Assignment of Case Numbers

1. Dispatch personnel who become aware of an incident occurring within the university service area that requires the initiation of police activity will assign an incident number generated by the CAD (Computer Aided Dispatch) system. Personnel must document law enforcement actions using either an incident, supplement, and/or crash reports (IACLEA 16.1.1c).

2. Case numbers will be assigned in numerical order and are unique to each incident.

3. Other reports, such as an accident, impoundment, property and evidence recovery, etc., will be assigned a CAD incident number (IACLEA 16.1.3).

4. When an incident is assigned a CAD number, the following information regarding that incident will be entered into the CAD system by dispatch personnel:
   a. Date and time of the initial reporting;
   b. Name and address of the complainant or victim requesting the service;
   c. Nature of the incident and the location;
   d. Identification of the officers assigned to the call;
   e. Time when officers were dispatched, arrived, and returned to service; and
   f. Status, date, and time of action taken on the call (IACLEA 16.1.1b).

C. Officer's Responsibilities

1. Officers will complete all required reports and turn them in to a supervisor prior to ending their shift (IACLEA 16.1.1d).

2. Officers shall provide only a short summary narrative of the event on the first page of the offense or incident report (who, what, when, and where). Details,

including any listing of evidence, identification of witnesses, description of injuries, and any exculpatory information, shall be provided in an offense or incident supplemental report.

3. Supervisors will review all reports for accuracy and completeness and submit completed reports to the records or CID units before the end of shift (IACLEA 16.1.1e).

4. Reports returned to officers for correction will be documented by the supervisor. At the next shift, the supervisor shall follow up and make sure that the report has been corrected and submitted.

D. Master Name Index

The dispatch supervisor will cause a master name index to be established, maintained, and updated. The index will be an alphabetical index of the names of persons identified in the field reports as complainants, arrestees, victims, witnesses, or suspects (IACLEA 16.1.5).

E. Juvenile Records (**TBP 10.02 f**)

1. A file is maintained on each juvenile (ages 10 to under 17) arrested, referred, or detained by an officer. The CAD system identifies juvenile records based on date of births, and once identified the reporting system flashes "Juvenile" across the record. The file includes all documents associated with the contact as indicated in this section, as well as a running list of the juvenile's detentions and dispositions.

2. State and federal laws require that juvenile files be kept separate from adult files.

3. Juvenile fingerprints and photographs, if any, will be turned over to the Juvenile Probation Department intake officer.

4. Police records will not maintain fingerprints or photographs of juveniles. Should fingerprints or photographs be turned over to police records they will be destroyed as specified in the Family Code sections 58.001 and 58.002.

F. Computerized Criminal History Information

1. Computerized criminal history information (CCH) is a federal/state cooperative system of a variety of databases (arrests, convictions, driving records, outstanding warrants, and others). The CCH database lists all arrests and convictions for offenses above Class C misdemeanor that have not been purged in accordance with state/federal age purge criteria.

2. Access to the TCIC/NCIC criminal history database is limited to designated personnel. The program generates its own log showing who accessed the system. The log is computerized and maintained by the Terminal Agency Coordinator.

3. Access to CCH information through local law enforcement agencies is limited to criminal justice uses.

4. No CCH will be released to non-government agencies or individuals (IACLEA 16.2.3).

5. Individuals who request a copy of their computerized criminal history must do so through the Texas Department of Public Safety in Austin.

6. Numerous agencies have been given authority to access criminal history information on prospective licensees or applicants. The statutes giving this authorization do not permit use of local police agency TCIC/NCIC lines for obtaining the CCH. Requests of this nature are to be referred to a supervisor.

VI. REPORT NUMBER AUDIT AND REPORT STATUS

A. Shift supervisors are required to review daily all report approval notifications maintained in the department's Reports Management System (RMS) to ensure that all reports from their squads have been turned in to the record's department. As documents are received, the reports will be saved as a data base service number.

B. When a report has not been turned in within three days of the incident, an email notification (reminder) will be sent to the officer for a response. Follow-ups for missing reports will be made daily until all missing reports are accounted for.

C. When a report has not been received within 72 hours after the end of the shift on which the call was taken, a missing-report notice will be sent to the officer and to the Patrol Lieutenant (IACLEA 16.1.4).

VII. DISTRIBUTION OF REPORTS AND RECORDS

A. After reviewing the reports for completeness, the patrol supervisor will forward all reports and citations to the records or CID unit.

B. All offense/incident reports will be maintained in the database for the required retention period. CID personnel will receive notification for all follow-up investigations.

C. Originals are maintained in the RMS system and/or record's management room.

D. All corrections or amendments to an original report that has been approved by a supervisor must be made by supplement and not by changing the original report. Supplementary reports will be maintained in the RMS database and/or record's management room (IACLEA 16.1.9).

E. Citations are entered into the computer system and forwarded to the appropriate court.

F. Field interview cards are entered into RMS by dispatchers and the cards are forwarded and maintained by CID.

G. Requests for and distribution of offense reports from SFASU University officials or other outside entities, including law enforcement, must be approved by the Chief of Police or his/her designee (IACLEA 16.2.1a).

H. Reports distributed to any law enforcement agency will be accompanied by all pertinent attachments and must be approved for release by the Chief of Police or his/her designee (IACLEA 16.2.1b).

I. All external requests for reports, including those from outside law enforcement agencies, departments within the institution, insurance companies, background investigators, and the public etc., will be in writing, emailed, or faxed. The request will be forwarded to the Records Manager for processing (IACLEA 16.2.1b, c, d & e).

VIII. RECORDS RETENTION AND DESTRUCTION (TBP 5.02)

A. Records will be retained in the records unit as specified in this policy until they are purged or destroyed in accordance with the approved University Records Retention Policy and any court orders requiring them to be expunged.

B. Accident Reports: Files will be maintained incident number. A copy of each accident report will be kept for two years, at which point they will be destroyed. Persons wanting accident reports older than two years can order a copy directly from the Texas Department of Public Safety.

C. Offense Reports: Because the limitations period for some offenses is based on the age of the victim at the time of the offense, offense report purging cannot be based solely on a calculation of the number of years from the date of the offense. Careful consideration will be given to these circumstances during the records retention process.

D. All Other Information Reports: The originals of miscellaneous incident reports will be kept according to the University's records retention policy. The records will be maintained in the RMS database.

E. Adult Arrest Files: Adults may obtain a court order to have their arrest records expunged as specified in Chapter 55 of the Code of Criminal Procedure. If no such order is obtained, adult arrest files will be maintained according to the University's records retention policy (IACLEA 16.1.7).

F. Juvenile Arrest Files: (**TBP 10.02 f**)

1. A juvenile arrest file will be created for every juvenile taken into custody by members of this department. Juvenile files are maintained separately from adult files and, like all files, are kept secure from unauthorized disclosure.

2. Persons may have their juvenile records sealed (not destroyed) by court order as specified in Family Code section 58.003.

3. A court may order destruction of juvenile detention files as specified in Family Code section 58.006.

4. Arrest report files on juveniles who were referred to juvenile court may be purged after the person reaches the age of 23.

5. Arrest report files on juveniles who were not referred to the juvenile court may be purged after the person reaches the age of 18.

6. As specified in Chapter 58 of the Family Code, police records will not maintain fingerprints or photographs of juveniles because the juvenile was detained by police or suspected of a criminal offense. Fingerprints and photographs taken as part of the juvenile intake process will be turned over to juvenile probation department officials. Should it happen that fingerprints or photographs have been turned over to police records, they will be destroyed as specified in Family Code sections 58.001 and 58.002.

7. Any juvenile records that are in a gang or criminal street gang intelligence file will be maintained, managed, and removed pursuant to the Texas Code of Criminal Procedure Articles 61.04 and 61.07.

G. Destruction of files and records will be done by shredding, burning, or other means of destruction approved by the police records supervisor and the records coordinator for the University when documents have been held beyond the required retention schedule.

IX. NATIONAL INCIDENT BASED REPORTING SYSTEM (NIBRS) AND RELEASE OF RECORDS

A. It is the responsibility of all law enforcement personnel to accurately enter the proper data into the NIBRS templates of the department's RMS system. Personnel must follow the instructions listed below:

1. Officers must electronically enter all applicable NIBRS information into the RMS reporting system.

2. The RMS reporting system is designed to perform a self-audit based on the information entered to verify all necessary data has been completed for the specific type of crime identified by the officer.

3. Once the officer has an error free report based on information entered, the report is automatically forwarded to a shift supervisor for review.

4. Supervisors are responsible to review all reports and to verify that the proper information has been entered into the system. Once verification has

occurred, the case is either forwarded to CID for follow-up or the data is compilation by the system.

5. Monthly, the CID Supervisor will use the RMS reporting system to compile data for Clery and NIBRS reporting.

6. NIBRS data forwarded to the state of Texas is sent electronically and is either accepted or rejected. Rejected data must be corrected by the CID Supervisor and resubmitted for approval (IACLEA 16.2.2).

B. The CID supervisor must read and be familiar with the NIBRS handbook, including all reporting standards.

C. The CID supervisor must perform several audit checks for each crime reported.

D. The Texas Public Information Act governs release of information reported to law enforcement agencies.

E. Any request for information contained in any report made or compiled by the department is to be referred to the CID unit.

F. All arrest files maintained in the records files and the computer will be the responsibility of the records supervisor and/or dispatch supervisor. Copies of files will be released only to the following authorized persons:

1. Personnel of this department
2. Sworn officers from other agencies upon written request
3. Courts of law under proper process
4. District / County attorneys
5. Federal law enforcement agencies
6. Probation departments
7. Military personnel with a written request and signed waiver of the named person. Copies of waivers will be kept for a period of three (3) years.

G. Juvenile arrest information is closed to public information requests and will not be released without a court order or signed waiver from the juvenile and a parent or guardian.

H. Original reports will be released only to members of this department. Every release will be documented in the records check-out log, showing the date, name, file name and number, and the name of the clerk releasing the files. A copy of the report will be maintained prior to release of any original report. Upon the return of original records, the records clerk will review the contents of the return against the "check-out log," checking for discrepancies. The records clerk will note who returned the files, as well as the date and time. If there are no discrepancies in the contents of the records being checked in, the receiving person will initial the "check-out log" and return the record to its original file location.

I. Records personnel will respond to all requests from the courts for original records. A complete copy of the requested records will be maintained before they are removed from the original records unit.

J. Any individual may request a "clearance letter" for a number of purposes, such as travel visas and adoptions. Such a letter must be submitted to records personnel along with at least two pieces of identification, one of which must include a photo. Records personnel will check local records only. Records personnel will prepare a "To Whom It May Concern" letter indicating that no criminal record has been recorded at the Stephen F. Austin State University Police Department. The individual makes state or federal criminal history inquiries directly to those agencies (**TBP 5.03**).

X. ANNUAL FIRE SAFETY AND SECURITY REPORT

A. The Annual Fire Safety and Security Report (AFSSR) is prepared by the Clery Compliance Manager and shall comply with all Clery Act requirements, as described in the Department of Education Handbook for Campus Safety and Security Handbook.

B. The Clery Compliance Manager is responsible for collecting, classifying and counting crime reports, crime statistics, and disciplinary referrals for crimes as specified in the Clery Act, including hate crimes, that occur:
   1. on campus
   2. in campus residential housing facilities
   3. within public property, including thoroughfares, streets, sidewalks, and parking facilities, that is within the campus or immediately adjacent to and accessible from the campus
   4. On certain non-campus property

C. These crimes include:
    1. Murder & Non-negligent manslaughter
    2. Manslaughter by Negligence
    3. Sexual Assault Offenses:
        i. Rape
        ii. Fondling
        iii. Incest
        iv. Statutory Rape
    4. Robbery
    5. Aggravated Assault
    6. Burglary
    7. Motor Vehicle Theft
    8. Arrests (Drug, Liquor, and Weapons Violations)
    9. Referrals for Disciplinary Action (Drug, Liquor, and Weapons Violations)

D. The Clery Compliance Manager will ensure that the Annual Fire Safety and Security Report, containing safety and security policy statements and crime statistics for the last three years, is published and distributed to all current students and employees no later than October First each year. This is accomplished by email and by posting the report on the UPD website.

E. The Clery Compliance Manager will submit crime statistics annually to the Department of Education via a web-based data collection process.

F. The Annual Fire Safety and Security Report is disseminated to personnel annually upon the approval of the Clery Compliance Manager (IACLEA 16.3.1a & b).

G. UPD will assist the Clery Compliance Manager by:
    1. Providing access to the RMS records management system;
    2. Assist as needed to properly classify reports;
    3. Assist the classification process by documenting the Clery geography in the narrative of each report;
    4. Supplying all required policies for the annual report which UPD is responsible for; and
    5. Assist in procuring crime statistics from other law enforcement agencies.

H. Definitions

1. Annual Fire Safety and Security Report: The Annual Fire Safety and Security Report is a document required to be published no later than October 1st of each year that provides crime statistics for the prior three years, policy statements regarding various safety and security measures, campus crime prevention program descriptions, and procedures to be followed in the investigation and prosecution of alleged sex offenses.

2. Clery Compliance Manager: The Clery Compliance Manager is designated by the Chief Compliance Officer and is responsible for compiling annual crime statistics, submitting annual crime statistics to the Department of Education, distributing the Stephen F. Austin State University Annual Fire Safety and Security Report, assisting with daily crime log compliance, and ensuring the University remains compliant with all requirements of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act).