


# FORT SMITH POLICE DEPARTMENT

## POLICIES AND PROCEDURES

SUBJECT	Criminal Intelligence		
NUMBER	1102.29	EFFECTIVE DATE	February 5, 2003
Scheduled Review Date	Annually beginning February 1	ISSUE DATE	February 5, 2003
REVIEW DATE		REVISION DATE	February 27, 2019
APPROVED BY		CALEA STANDARDS	LE40.2.3: LE40.2.1; LE40.2.2

### I. Purpose and Scope

- A. The purpose of this policy is to establish procedures regulating the collection, storage, and dissemination of criminal intelligence information by members of the Fort Smith Police Department.
- B. This policy shall apply to all members of the Fort Smith Police Department.

### II. Policy [LE 42.1.6.a]

- A. The Fort Smith Police Department recognizes that the gathering of intelligence information, to include the evaluation, dissemination, and security of such information, is an important aspect of the law enforcement function. All members are encouraged to develop and gather effective and lawful intelligence data whenever appropriate.
- B. Individuals or groups known to be or suspected of being involved in criminal acts, or who are known to be or suspected of being involved in the threatening, planning, organizing, or financing of criminal acts shall be considered a threat to the community. It shall be the policy of the Fort Smith Police Department to maintain a criminal intelligence function, the purpose of which is to collect and analyze information on groups and individuals who are known to be or suspected of being involved in activities that present a threat to the community.
- C. All information determined to be criminal intelligence shall be maintained in the Fort Smith Police Department's CrimeNtel Intelligence database.

### III. Procedures

- A. The criminal intelligence function is a component of the Criminal Investigations Division, and shall be under the direct command of the Criminal Investigations Division Commander.
- B. Members of the Fort Smith Police Department and departmental equipment may be used as necessary for the collection of raw data, strategic intelligence, tactical intelligence, and as support for legitimate overt and covert law enforcement operations. *Criminal intelligence shall in no way be used to collect information for any reasons not specifically related to crime or suspected criminal activity.*

Page 1 of 7	Effective Date: February 5, 2003
Subject: Criminal Intelligence	Number: 1102.29

- C. To ensure the legality and integrity of its operations, information is only to be gathered relative to legitimate investigative objectives relating to the control and prevention of criminal conduct, and activities that present a threat to the community.
- D. The collection of intelligence information shall be strictly limited to information concerning individuals or groups known to, or suspected of, threatening, planning, organizing, financing or committing criminal activities that constitute a threat to this community. Examples of such criminal activity include but are not limited to:
1. Organized crime activity
  2. Illegal drug activity
  3. Vice related activity
  4. Terrorism
  5. Gang related activity
  6. Activities promoting community unrest
  7. Or other activity that poses a potential threat to the community.
- E. The submitting officer shall rate the quality of the information that is being entered into the criminal intelligence database utilizing the following criteria:
1. Information Source
    - a. Source name. The source is the individual from which the information originated. The source should not be the police officer to whom the information was provided unless that police officer is the originating source. The name of the source should be included when possible. When the name of the source is unknown, a source name of "Anonymous Source" should be entered.
    - b. Source reliability. The submitting officer shall establish the reliability of the source. When attempting to establish the reliability of the source, the submitting officer shall take into account such traits as prior reliability, motivation, knowledge of specific crime and/or any other factor known to credit or discredit the reliability of a witness. The reliability of the source shall be rated as follows:
      - (1) Completely Reliable
      - (2) Usually Reliable
      - (3) Unknown Reliability
      - (4) Not Reliable
- Any source listed as "Anonymous Source" must be rated as "Unknown Reliability". *Any information provided by a source that is rated at any time as "Not Reliable" shall not be entered into the intelligence database for longer than thirty (30) days unless the information supplied is confirmed.*

Page 2 of 7	Effective Date: February 5, 2003
Subject: Criminal Intelligence	Number: 1102.29

- c. Source confidentiality. Any source classified as a Confidential Informant in accordance with FSPD Policy and Procedure #1102.13 shall be indicated as such in the appropriate field of the CrimeNtel source submission. Additionally, the Confidential Informant's control number, as provided by the Master File of Informant Information maintenance supervisor, shall be included. All Confidential Informant sources shall have a source access level of Top Secret.
- d. Source access level. The submitting officer shall establish the access level for his or her source. Access levels establish which officers may have access to source names and intelligence information. Access levels are "top down", meaning information is accessible by an individual at their rated level and below. Unless specified herein, access levels for individual officers shall be at the discretion of the CID Division Commander or his designee. Access levels may be raised or lowered to accommodate special or temporary assignments. The access levels are classified as follows:
  - (1) Top Secret- Sources or intelligence information classified as "Top Secret" may only be accessed by the Chief of Police, the CID Division Commander or his/her designated intelligence maintenance supervisor(s). *No source or intelligence information shall be rated as "Top Secret" without approval from the Chief of Police, the CID Division Commander, or the intelligence maintenance supervisor(s).* Top Secret information may not be released to anyone without Top Secret clearance.
  - (2) Secret- Sources or intelligence information classified as "Secret" are accessible by select individuals assigned to units with the most "need to know". This includes, but may not be limited to the Narcotics/Intelligence units and certain CID supervisors. Secret information may be released ONLY to sworn FSPD personnel with a specific "need to know" standing.
  - (3) Confidential- Sources or intelligence information classified as "Confidential" are accessible by all sworn Fort Smith Police Department personnel with access to the CrimeNtel database and may be released ONLY to sworn FSPD personnel.
  - (4) Restricted- Sources or intelligence information classified as "Restricted" are accessible by all sworn law enforcement personnel, regardless of agency, with access to the FSPD CrimeNtel database and may be released to any law enforcement officer regardless of agency.
  - (5) Unclassified- Sources or intelligence information classified as "Unclassified" may be released to non-law enforcement personnel.

## 2. Information Validity

- a. The submitting officer shall judge the validity of the intelligence information by one of the following standards:

### (1) Confirmed

Page 3 of 7	Effective Date: February 5, 2003
Subject: Criminal Intelligence	Number: 1102.29

- (2) Probable
- (3) Doubtful
- (4) Cannot Be Judged

### 3. Information Access Level

- a. The submitting officer shall determine the information access level using the standards and criteria as outlined in the source access level portion of this policy (section E.1.d):

- (1) Top Secret
- (2) Secret
- (3) Confidential
- (4) Restricted
- (5) Unclassified

### 4. Information Retention Level

- a. The submitting officer shall determine the information retention level based upon the Source Reliability and Information Validity ratings. Following are the allowed retention schedules:

- (1) Permanent (5 years)
- (2) Interim (2 years)
- (3) Temporary (30 days)

- b. When determining the information retention level, the submitting officer should weigh both the reliability of their source along with the validity of the information provided. Information which is judged to reach the level of *reasonable suspicion or beyond* and having a high likelihood of still being valid in several years may be retained for a period of five (5) years. Information judged to reach a level of *reasonable suspicion* but which will likely no longer be valid in five years may be retained for a period of two (2) years. Any information with a level of proof less than *reasonable suspicion* may only be retained for a period of thirty (30) days.

- c. For the purposes of this policy, *reasonable suspicion* shall be defined as *a suspicion based on facts or circumstances which of themselves do not give rise to the probable cause requisite to justify a lawful arrest, but which give rise to more than a bare suspicion; that is, a suspicion that is reasonable as opposed to imaginary or conjectural suspicion.*

- d. Information which is judged to have less than reasonable suspicion, such as a bare suspicion, mere hunch, or unsubstantiated complaint, may be entered into the CrimeNtel database on a temporary basis. Such information must be given a retention setting of thirty (30) days and must

Page 4 of 7	Effective Date: February 5, 2003
Subject: Criminal Intelligence	Number: 1102.29

not be disseminated outside the FSPD. Upon submission, the reviewing supervisor should assign such temporary information to an investigator for follow-up. If, within thirty (30) days, new facts or circumstances are developed which substantiate or raise the validity level of the original information to *reasonable suspicion*, the retention schedule may then be changed to Interim or Permanent. The investigator(s) assigned to follow up on a submission shall document their investigative findings in the narrative portion of the CrimeNtel record. Any temporary information which is not investigated or validated in some way shall be purged from the database after thirty (30) days.

#### 5. Criminal Activity Type

- a. The submitting officer shall identify the specific criminal activity type for which the information pertains to.
- F. Prior to entry into the CrimeNtel database, the Criminal Investigations Division Commander, or his/her designee(s), shall review the information to ensure that it is collected in compliance with this policy and applicable laws. If necessary, the reviewing supervisor shall contact the submitting officer to gather additional information that may be needed to facilitate entry into the database. The reviewing supervisor may, at his or her discretion, change the submitting officer's rating of the information validity, information access level, and information retention level based on his or her own judgment of the information. *Information that is not in compliance shall not be entered into the system. The criminal intelligence function shall in no way be utilized to collect information for any reasons not related to crime or suspected criminal activity.*
- G. The Criminal Investigations Division Commander, or his/her designee, will ensure that intelligence information that is out of date or no longer serves a valid informational source is purged from the system in accordance with the following procedures:
  - 1. All intelligence files on suspected criminals and criminal activity shall be reviewed by the CID Commander and his/her staff. File reviews shall take place as close to the purge/review date established by the original retention schedule as possible. Records shall be purged when no new information has been received which would indicate continued criminal activity or the possibility of continued criminal activity in the future. Should it be determined at the time of review that new information indicates *reasonable suspicion* of continued criminal activity; a new purge/review date shall be established, based on the source reliability and validity of the new information.
- H. Officers wishing to submit information for possible entry into the intelligence system should reduce the information to writing and forward it to the CID Commander or to the appropriate CID supervisor to which the information pertains. Electronic submissions (such as email) are the preferred methods of submission. After the information is entered into the CrimeNtel data base, any original submission forms shall be destroyed.
- I. The CID Commander, or his/her designee(s), shall review the information to determine whether it should be entered into the CrimeNtel database. No information will be entered into the system without the approval of the CID Commander, or his/her designee(s).
- J. Only those intelligence files that have a level rating of "Unclassified" or "Restricted" may be disseminated to personnel who are not employed by the Fort Smith Police Department. Intelligence files that have a level rating of "Confidential", "Secret" and "Top Secret" may **only** be released to members of the Fort Smith Police Department. In all cases, information shall be disseminated on a "need to know" basis.

Page 5 of 7	Effective Date: February 5, 2003
Subject: Criminal Intelligence	Number: 1102.29

- K. Any officer who disseminates any information from any intelligence record in the CrimeNtel database must immediately complete the dissemination history portion of the respective CrimeNtel intelligence record(s), indicating the date of release, the dissemination type, the name of the releasing officer, the name (and agency if applicable) of the recipient, why the information was disseminated, the nature of the information given, and the case or file number of the intelligence record.
- L. The selection of personnel that may be needed for the gathering of intelligence information shall be the responsibility of the CID Commander. The CID Commander shall ensure that personnel utilized shall be familiar with intelligence gathering techniques. Additionally, personnel shall be familiar with any specialized equipment that may be required. Procedures governing the operation of this equipment are located in FSPD Policy and Procedure # 1106.07.
- M. Every three (3) years, the Training Coordinator will ensure all personnel review and receive instruction on this agency's policies and procedures relating to the collection, processing and sharing of intelligence information and information regarding suspicious activity that presents a threat to the community.
- N. An annual documented review of procedures and processes will be conducted by the Criminal Investigations Division Commander or his designee.

#### IV. File Security

- A. Access to the *inquiry* function of the CrimeNtel database shall be limited to those persons authorized by the Criminal Investigations Division Commander. Such access will be facilitated by a modification to the officer's access privileges granting "permission" for that purpose.
- B. Access to the *entry and modification* functions shall be restricted to the Criminal Investigations Division Commander, or his designated supervisor(s), the clerk assigned to the Narcotics Unit, or to other personnel as authorized by the CID Division Commander. All submissions made directly into the CrimeNtel database by personnel other than the Chief of Police, the CID Division Commander or his/her designated supervisor(s) shall be automatically placed into an electronic "holding bin" where it shall reside until reviewed by the appropriate CID supervisor(s). Only upon review and release from the electronic holding bin by a CID supervisor will the information become part of the CrimeNtel database.
- C. Access to the *purge* functions shall be restricted to the Criminal Investigations Division Commander or his designated supervisor(s).
- D. In instances where an intelligence record includes documentation such as photographs, newspaper articles, web pages, e-mail attachments, etc., the documents shall be included with the appropriate record in the CrimeNtel database in digital format.

#### V. Gang Information

- A. Before any individual may be identified with a criminal gang or organization in the CrimeNtel database, certain traits specific to that gang or organization must be attributed to the individual. These traits or characteristics are divided into two categories: *Hard Identifiers* and *Soft Identifiers*. For inclusion in the CrimeNtel database as a gang member, at least one (1) Hard Identifier or at least two (2) Soft Identifiers must be identified and associated with the individual.

Page 6 of 7	Effective Date: February 5, 2003
Subject: Criminal Intelligence	Number: 1102.29

1. Hard Identifiers:
  - a. Self-Admittance
  - b. Gang Specific Tattoos
  - c. Traditional Gang Symbols
  - d. Specific Gang Graffiti
  - e. Gang Specific Patches/Logos
2. Soft Identifiers (include but are not limited to):
  - a. Colors
  - b. Clothing styles
  - c. Clothing accessories/jewelry
  - d. Methods of wearing clothes/colors (Left or Right side, etc.)
  - e. Traditional gang numbers (ex: 13, XII, 14, XIV, etc.)
  - f. Association with other known gang members
  - g. Hand signs
  - h. Gang slang
  - i. Specific hair/eyebrow markings
  - j. Presence at known gang clubhouse/establishment

B. All hard and/or soft identifiers used to associate an individual with a criminal gang must be articulated within the narrative portion of the CrimeNtel record for that individual. Submissions lacking at least one (1) hard identifier or two (2) soft identifiers will not be retained.

## **VI. Non-Criminal Information**

- A. As stated in Section III.B of this policy: *Criminal intelligence shall in no way be used to collect information for any reasons not specifically related to crime or suspected criminal activity.* In certain instances, the use of the name of a person, group, business, or organization suspected of *no criminal activity* is necessary in articulating the actual intelligence information. Such an example would be providing the name of the source in the narrative of the record. Though the person named is not suspected of any criminal activity, their identification is necessary for future investigative follow-up. In such instances, those persons, groups, businesses, or organizations named in an intelligence record which are under no suspicion of wrong doing shall be clearly identified in writing with the acronym “NCIP” for “Non Criminal Information Purposes”.

Page 7 of 7	Effective Date: February 5, 2003
Subject: Criminal Intelligence	Number: 1102.29