PURPOSE:

This policy establishes guidelines for collecting, processing, and disseminating information relating to specified crimes and criminal activities. Areas of concern typically include organized crime, vice, illegal drug trafficking, terrorism, gangs, and civil disorders.

CRIMINAL INTELLIGENCE:

DEFINED – The end product of a process that converts individual items of information either into evidence or, more often, into insights conclusion, or assessments, perhaps less solid than fact but always more helpful than raw information, that can form the basis for the development of law enforcement strategies, priorities, policies, or investigative tactics regarding specific crime, suspect, criminal organization, etc. The intelligence process includes the systematic collection of raw information, which after collation, evaluation, and analysis, is disseminated to appropriate units of the agency.

CRIMINAL INTELLIGENCE ACCOUNTABILITY:

Vice and Narcotics is the central repository for intelligence records. The Division Commander evaluates intelligence information, and arranges meetings to share and analyze information with affected Division Commanders, unit supervisors and investigators as needed.

The Division Commander of any Sheriff's Office component or function that gathers intelligence information is responsible for that activity within his division including compiling, initial evaluation and accountability of records. Intelligence records are then forwarded to Vice and Narcotics.

All sworn personnel will receive training in Intelligence Lead Sheets and those personnel tasked with intelligence operations will receive additional training.

It is the responsibility of all agency personnel to forward potential criminal intelligence through the chain of command to Vice and Narcotics.

CRIMINAL INTELLIGENCE FILES:

A criminal intelligence file consists of stored information on the activities and associations of individuals and groups known or suspected to be involved in criminal acts or in the threatening, planning, organizing or financing of criminal acts.
More specifically, this stored information relates to individuals who fall into one or more of the following:

1. Are currently involved in or suspected of being involved in the planning, organizing, financing, or commission of criminal activities.
2. Have threatened, attempted, planned, or performed criminal acts.

Have an established association with known or suspected crime figures. Organizations and businesses involved in one or more of the following:

1. Are currently involved in or suspected of being involved in the planning, organizing, financing, or commission of criminal activities; or
2. Which have threatened, attempted, planned, or performed criminal acts; or
3. Are operated, controlled, financed, infiltrated or illegally used by crime fighters.

CRIMINAL INTELLIGENCE FILE CONTENT:

Material stored in a criminal intelligence file is restricted to documents of criminal intelligence and related information from public records and media sources. Examples of excluded material are religious, political, or sexual information not relating to criminal conduct and associations with individuals not of a criminal nature.

CRIMINAL INTELLIGENCE FILE CRITERIA:

Criminal intelligences consist of two specific categories: permanent files and temporary files.

PERMANENT FILE – A file containing information pertaining to an identifiable subject meeting the following criteria justified for retention in a permanent criminal intelligence file:

1. Information which relates that an individual, organization, business or group is involved or suspected of being involved in one or more of the following criminal activities:
    - Narcotics trafficking.
    - Unlawful gambling.
    - Loan sharking.
    - Extortion.
    - Vice and pornography.
    - Infiltration of legitimate business for illegitimate purposes.
    - Stolen securities.
    - Bribery.
    - Threats to public officials and private citizens.
    - Major fencing activities.

- Major crime including homicide, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, forgery, and arson.
- Manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, or political motivation.

2. In addition to falling within the confines of one or more of the previously listed criminal activities, the subject entered into the permanent file is identifiable – distinguished by a unique identifying characteristic, e.g., date of birth, criminal identification number, or driver's license number. Identification at the time of file input is necessary to distinguish the subject from any similar individuals on file or any others to be entered at a later time.

TEMPORARY FILE – Information in file does not meet criteria for permanent file storage but has enough potential validity for the agency to want to retain it. It is recommended that retention of information in a temporary file not to exceed a one-year period unless compelling reason exists to extend this time period. During this period, efforts are to be made to identify the subject or validate the information so it may be transferred to the permanent file or destroyed. If the information still remains in the temporary file at the end of the one-year period, and compelling reason for its retention is not evident, the information is to be removed and destroyed. An individual, organization, business, or group may be given temporary file status in the following cases:

1. **Subject is unidentifiable-** Although suspected of involvement in criminal activities, the subject has no physical descriptors, identification numbers, or distinguishing characteristics available.
2. **Involvement is questionable-** Subject's involvement in criminal activities is questionable; however, based on one or both of the following reasons it would be beneficial to the agency to retain a record of the subject for a limited period of time during which the information can be validated.
3. **Possible criminal association-** Individual or organization, although not currently reported to be criminally active, associates with a known criminal and appears to be aided by abetting illegal activities.

4. **Criminal history**- Individual or organization, although not currently reported to be criminally active, has a history of criminal conduct and the circumstances currently being reported, i.e., new position or ownership in a business, affords an opportunity to again become criminally active.
5. **Reliability/validity unknown- The** reliability of the information source and/or the validity of the information cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while attempts are made to validate.

CRIMINAL INTELLIGENCE INFORMATION EVALUATION:

Information retained in a criminal intelligence file is to be evaluated for source reliability and content validity prior to filing. The bulk of data in an intelligence file consists of allegations or information initially unverified. Evaluating the information's worth and usefulness is essential in protecting an individual's right of privacy. Circulating unreliable and invalid information is detrimental to agency's operations and contrary to an individual's right of privacy.

To ensure uniformity, the following terms describe language to be used in the evaluation process:

Source Reliability –

1. **Reliable**- The reliability of the source is unquestioned or has been well tested in the past.
2. **Usually Reliable**- The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.
3. **Unreliable**- The reliability of the source has been sporadic in the past.
4. **Unknown-** The reliability of the source cannot be judged. Its authenticity of trustworthiness has not yet been determined by either experience or investigation.

Content Validity –

1. **Confirmed-** The information has been corroborated.
2. **Probable**- The information is consistent with past accounts.
3. **Doubtful**- The information is inconsistent with past accounts.
4. **Cannot be judged**- The information cannot be evaluated.

FILE EVALUATION CODING SYSTEM - The following codes are to be noted on all file information to describe source reliability and content validity:

1. Source Reliability - Note file information as: **RELIABLE, USUALLY RELIABLE, UNRELIABLE, OR UNKNOWN**.

2. Content Validity – Note file information as: **CONFIRMED, PROBABLE, DOUBTFUL, OR CANNOT BE JUDGED**.

CRIMINAL INTELLIGENCE INFORMATION AND DISSEMINATION

CLASSIFICATION: Information classification is the responsibility of a carefully selected and specifically designated individual in the effected operational unit. Information retained in a criminal intelligence file is to be classified to indicate the degree to which it will be kept confidential in order to protect sources, investigations, and an individual's right of privacy. Additionally, classification dictates the internal approval process to be completed prior to dissemination of the information to personnel outside the Sheriff's Office.

In order to ensure uniformity, the following diagrams the system to be used for classifying criminal intelligence files:

Security Class	Dissemination Criteria	Release Authority
Class I Confidential	Restricted to law enforcement intelligence personnel having a specific need-to-know and right-to-know	Division Commander
Class II Sensitive	Restricted to law enforcement intelligence personnel having a specific need-to-know and right-to-know	Unit Commander
Class III Restricted	Restricted to law enforcement personnel having a specific need-to-know and right-to-know	Unit Supervisor

DISSEMINATION - In order to protect the right of privacy of individuals contained in criminal intelligence files and to maintain confidentiality of sources and the file itself, the following applies to file dissemination:

1. **NEED-TO-KNOW**. Requested information is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation.
2. **RIGHT-TO-KNOW**. Requesting agency has official capacity and statutory authority to the information requested.

To eliminate unauthorized use and abuse of criminal intelligence information, the following documentation is to be noted in disseminated files:

1. The name of the agency and individual requesting the information.

2. The need-to-know clearly defined.
3. The information provided.
4. The name of the employee handling the request.

Examples of classified information:

Class I – Confidential

- Information pertaining to law enforcement cases currently under investigation.
- Corruption (police or other government officials).
- Informant identification information.

Class II – Sensitive

- Criminal intelligence reports that refer to organized crime or terrorism.
- Publications obtained through intelligence unit channels not deemed to be confidential.

Class III – Restricted

- Reports that at an earlier date were classified confidential or sensitive, and the need for high security no longer exist.
- Non-sensitive reports published by local law enforcement agencies.

DISSEMINATION - Information determined to be of a useful nature to operational units is to be disseminated in a timely manner. Supervisors are to solicit feedback to evaluate information effectiveness.

CRIMINAL INTELLIGENCE INFORMATION SOURCES:

In a number of situations, the affected operational unit may elect to identify information sources for items stored in their criminal intelligence files. The value of information stored in a criminal intelligence file is often directly related to the source of the information.

Factors to consider in determining whether source identification is warranted include:

1. The nature of the information reported.
2. The potential need to refer to the source's identity for further investigative or prosecutorial activity.
3. The reliability of the source.

When source identification is warranted, it will reflect the name of the agency and the individual providing the information.

In cases where identifying the source is not practical for internal security reasons, a code number can be used. A listing of coded sources of information can then be retained by the operational unit commander. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information, e.g., "S-60, a reliable police informant, heard" or "a reliable law enforcement source of the Anderson County Sheriff's Office saw" a particular
event at a particular time.

In many cases there is no need to indicate the source of the stored information. However, each item of information is to be individually judged against established criteria to determine whether or not source identification is appropriate.

CRIMINAL INTELLIGENCE INFORMATION QUALITY CONTROL:

Information stored in a criminal intelligence file is to be reviewed for compliance with established policy guidelines filing. This quality control requirement is the responsibility of a carefully selected and specifically designated individual in the operational unit.

The quality control reviewer is responsible for ensuring all information entered into a criminal intelligence file conforms to policy criteria and is properly evaluated and classified. Review of file input ensures the quality of the criminal intelligence file in meeting policy requirements.

CRIMINAL INTELLIGENCE FILE PURGING:

Information stored in a criminal intelligence file is to be periodically reviewed and purged to ensure:

1. The file is current, accurate and relevant to the needs and objectives of the Sheriff's Office.
2. To safeguard an individual's rights of privacy as guaranteed under federal and state laws.

Reviewing of criminal intelligence is to be done on a continual basis as personnel use the material in carrying out day-to-day activities. Information that appears to be no longer useful or cannot be validated is to be immediately purged from a file and destroyed.

To ensure review and purge of a file is conducted systematically, the following table outlines considerations required in the purge/destruction process:

Utility	Timeliness and appropriateness	Accuracy and completeness
How often is the information used?	Is the information outdated?	Is the information still valid?
For what purpose is the information being used?	Is the information relevant to the needs and objectives of law enforcement?	Is the information adequate for identification purposes?
Who uses the information?	Is the information relevant to the purpose for which it was collected and stored?	Can the validity of the data be determined through investigative techniques?
	Is the information available from other sources?	
	Is this non-intelligence information that should be stored elsewhere?	
	Is the security classification assigned the information still appropriate?	

PURGE TIME SCHEDULE – Review of criminal intelligence files for purging is to be conducted on an annual basis.

MANNER OF DESTRUCTION – Material purged from criminal intelligence files is to be destroyed under the supervision of members of the affected Division Commander.

CRIMINAL INTELLIGENCE FILE SECURITY: Criminal intelligence files are to be located in a secure area with access restricted to authorized personnel. Physical security of criminal intelligence files is imperative to maintain confidentiality of the information stored and to ensure protection of an individual's right to privacy.

LIASON: To facilitate the effectiveness of intelligence gathering, the Sheriff's Office maintains a liaison with federal, state, and other local law enforcement agencies for the exchange of intelligence information.

DECONFLICTION: Event deconfliction is the process of determining when law enforcement personnel are conducting events in close proximity to one another at the same time. By notifying a central location of a planned event prior to its execution, officers will not knowingly target or conflict with another law enforcement officer or compromise another investigation. This is particularly important for agencies in concurrent or contiguous jurisdictions that are involved in high risk activities such as undercover operations, surveillances, execution of search warrants, or fugitive apprehensions.
When certain elements (e.g. location, date and time) are matched between two or more events/operations, a conflict (or hit) results. Immediate notification is then made by the deconfliction system to the involved agency personnel.

The event deconfliction process is a pointer system, alerting officers that they may be operating near one another.

When a conflict exists, both agencies are notified in order for them to determine the nature of the conflict and individually decide the extent to which they wish to share case details.

It is standard practice of the DEU to engage in event deconfliction in an attempt to avoid dangerous confrontations and/or unintentional consequences for law enforcement personnel and our citizens by entering qualifying events into the SafeTNet system. SafeTNet is a software system operated by the El Paso Intelligence Center (EPIC). SafeTNet is a recommended deconfliction software tool endorsed by CALEA as a model policy system. All information entered is considered confidential and law enforcement sensitive.

The following activities/events shall be entered into the event deconfliction system:
1. The service of search warrants;
2. The service of arrest warrants;
3. The planned arrest of a person immediately after he or she has delivered or received, or attempted to deliver or receive, contraband to or from an officer or informant (buy-busts, reverse sting operations, controlled drug deliveries, stolen or burglarized property, etc.);
4. Taking delivery of any contraband from a suspect who is not arrested, but permitted to leave pending further investigation ("buy-walk");
5. Informant or officer face-to-face meetings with suspects for the purpose of receiving, delivering, or negotiating the receipt or delivery of any contraband;
6. Approaching a person at his or her place of domicile and requesting permission to search for any contraband ("knock and talk"); especially in anticipation of activities involving a felony crime or drug related crime;
7. Predetermined surveillances, whether stationary or mobile, including those occurring in our agency's jurisdiction or the jurisdiction of a non-participating law enforcement agency;
8. Covert activity by officers, or by informants acting under the direction of officers, that could initiate a response from citizens or local police who may reasonably believe that a crime is in progress;
9. Fugitive operations which are operational (roundups);
10. Long term covert operations (storefronts);
11. Any other high-risk or specialized law enforcement activities that would benefit from event deconfliction.

DEU personnel conducting field operations as described above shall ensure that these operations are entered into the event deconfliction system.

All operations requiring entry into the event deconfliction system shall be made as soon as information is available, but should be made at least two hours prior to the event taking place, if possible.

Information entered into the deconfliction system shall include:
1. Date and time of planned operation;
2. Type of operation;
3. Location of the operation, including any staging areas;
4. Information about the suspect(s), including full names, aliases or monikers, date of birth, vehicle information, phone numbers, contraband to be purchased and amount of money involved;
5. Lead and participating agency names;
6. Name and agency of the person entering the operation, including cellular telephone number, along with a secondary point of contact for the operation.
7. Specify the radius of deconfliction (if not preset by the deconfliction system).

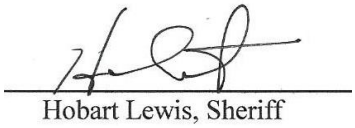
If a conflict with other law enforcement activity is identified through SafeTNet both of the contact personnel will be notified by the event deconfliction system. Each affected law enforcement entity is responsible for contacting one another and resolving the conflict before taking further action. Investigating personnel must refrain from executing any operations until identified conflicts have been resolved. Unresolved operational conflicts will be immediately referred to command/supervisory level personnel.

Any exemption or deviation from this procedure shall be considered on a case-by-case basis and approved only by a command/supervisory level officer.

Training and Access:
All personnel with assignments that may require them to perform event deconfliction shall receive training enabling them to obtain appropriate security access and to navigate through the event deconfliction system.

Event deconfliction is a key component of officer safety during planned police operations and high risk investigations. Consequently, failure to comply with this policy may result in disciplinary action.

ANNUAL REVIEW: An annual review of this policy will be conducted by the Accreditation Manager to ensure compliance and determine if any changes are to be made.



Hobart Lewis, Sheriff