Jason Bammann, Chief of Police

//J. Bammann// Date: _____

GENERAL ORDER 40

CRIME ANALYSIS PROCEDURES

EFFECTIVE DATE: March 22, 2024

SUMMARY OF REVISIONS:

INDEX OF STANDARDS

PURPOSE: The purpose of this chapter is to establish the principles of the crime analysis function to include data collection, evaluation, analysis and dissemination and how this information is used to effectively identify crime patterns and/or trends.

40.1 CRIME ANALYSIS

40.1.1 CRIME ANALYSIS PROCEDURES

A. Source documents: Crime analysis will be based on offense and case investigation reports, arrest summaries, call for service reports, citation reports, and crash reports. These source documents are located in the Computer-Aided Dispatch (CAD) system and CRIMES Record Management System (RMS).

Among the factors to be considered in crime analysis includes:

– Frequency by Type of Crime;

- Geographical or Spatial Factors;
- Chronological or Temporal Factors;
- Victim and Target Descriptors;
- Suspect Descriptors;
- Suspect Vehicle Descriptors;
- Modus Operandi Factors;
- Physical Evidence Information;
- Problem Oriented or Community Policing Strategies.

B. Evaluation of Collected Data: crime data information will be evaluated for accuracy using various analytical tools including spreadsheets, geographical information systems (GIS) and statistical software for accuracy.

C. Dissemination of information: Crime analysis information will be released in staff meetings, published on the intranet, and/or disseminated on an as-needed basis to affected personnel or functions. Information that is relevant to specific line units should be sent to them directly. Information that pertains to tactical or strategic plans should be provided to all affected units. Crime analysis that would enhance public information and generate public support may be disseminated to the community.

- **Feedback:** Recipients of crime analysis may provide feedback in the form of e-mail or other notifications.

D. Briefing the Chief: The Chief of Police will be briefed on crime patterns and trends through staff meetings and crime analysis reports forwarded to the Chief of Police.

40.2 INTELLIGENCE ANALYSES PROCEDURES

40.2.1 COLLECTION OF CRIMINAL INTELLIGENCE DATA

Collecting intelligence information: Intelligence activities of the Mansfield Division of Police shall include information gathering, processing, and dissemination of information relating only to criminal activity and/or threats to the community to the appropriate, authorized personnel. Such information includes "tips and leads".

The Special Investigative Section will safeguard the integrity of all intelligence files and ensure that legal requirements relating to such files are not compromised. This will include:

- **Ensuring the anonymity of all Sources**.
- Limiting the collection of intelligence information to criminal conduct and activities that present an identifiable threat to the community.
- Restricting activities to the collection of unconfirmed intelligence, strategic intelligence, and tactical intelligence. These forms of intelligence information are defined below:

- **Unconfirmed Intelligence:** Information from various sources (often anonymous) that by itself may infer criminal activity often referred to as tips and leads, but when combined with other information may legally establish criminal activity.

- **Strategic Intelligence:** Information that is gathered in response to a policing problem and which is used to direct police efforts to a specific area, criminal activity, or modus operandi in an attempt to determine criminal responsibility, arrest criminal offenders, and prevent additional crime occurrences. Strategic Intelligence is used for planning, problem-solving and assessments.

- **Tactical Intelligence:** Information that is gathered for use in the allocation of manpower and equipment to combat or suppress identified active criminal activity.

40.2.2 PROCEDURES FOR INTELLIGENCE ANALYSIS

A. Sources of intelligence information: Criminal intelligence sources can include offense and case investigation reports, Homeland Security alerts, state crime alerts, arrest summaries, call for service reports, citation reports, surveillance activities covert operations, etc.
Information to be included in an intelligence report shall be related to specified, suspected crimes and criminal activities, including vice and organized crime, drugs, terrorism, gangs, civil disorders, and routine criminal activity. This information may include simple tips and/or leads provided by anonymous sources. The Intelligence Report uses a source evaluation and content rating to ensure the quality of information.

B. All intelligence reports shall be screened by a Special Investigative Section supervisor or designated Intelligence Officer to ensure it is related to criminal activity and/or threats to the community during the coding process PRIOR to entry into the automated system.

- Information extracted from Intelligence Reports, except those specifically relating to restricted, covert or undercover investigations, may be distributed to all members of the Division through e-mail and/or MDT alert for Strategic or Tactical purposed upon approval of the SIS Commander or Intelligence Officer.

- Information related to covert or undercover operations shall be released on a need-to-know basis only, as determined by the Special Investigative Section Commander, Special Operation Bureau Commander and/or the Chief of Police.

40.2.3 PROCEDURES FOR CRIMINAL INTELLIGENCE (LE1)

A. It is the **responsibility** of ALL agency personnel to gather and properly document all relevant intelligence information. Personnel shall document known or suspected criminal information prior to the end of their tour of duty and forward same to the Special Investigative Section (SIS) for evaluation and storage. **Personnel shall document all intelligence information on an "Intelligence Report".**

- **All Division personnel will be trained** on the use of intelligence report forms and process and shall document information received as outlined in A, above.

- Utilization of personnel and techniques**:** Intelligence operations requiring the use of specific

personnel, specialized equipment, and/or special techniques requiring special training shall be at the direction of the Special Investigative Section or the Special Operations Bureau Commander or and/or the Chief of Police.

- Prior to the beginning of any intelligence operation, the investigating officer shall complete a written special operations plan, to be reviewed by the designated Section Commander and approved by the SIS Commander, Special Operations Bureau Commander, and/or the Chief of Police.

B. **Safe and Secure Storage of Information:** All designated Intelligence Reports and/or files of the Mansfield Division of Police will be maintained using procedures to safeguard the intelligence information in a secure safe manner to include storage in a secure location with controlled access and after-hours alarm system. The SIS Commander is responsible for maintaining the safety and security of such information. Dissemination of such information will also be controlled.

- Information contained in the intelligence database will have access limited to authorized agency personnel on a "need-to-know" and a "right-to-know" basis. (Requests for information submitted by collaborative agencies may result in a referral (Pointer System) to the submitting agency only).

- **"Need-to-know"** is defined as any law enforcement agency in the lawful pursuit of a criminal investigation; any law enforcement agency (including prosecution) preparing an assessment of criminal activity where this information is required; or any law enforcement agency developing an analytical product pertaining to strategic or tactical analysis.

- **"Right-to-know"** is defined as any law enforcement agency in the lawful pursuit of a "specific" criminal investigation.

Definitions:

- **"Criminal activity"** is defined as any activity that pertains to the commission, or possible commission of a crime.

- **"Threats to the community"** are defined as any information pertaining to any actual, perceived or potential threats to the health, safety and welfare of the community.

C. Requests, Inquiries and Dissemination of information will be documented and maintained on the Inquiry Log. Any breach of security in these or other agency files by departmental personnel may result in disciplinary action up to and including termination.

D. **Methods for purging information:** Information classified as intelligence as described in this section and entered in the intelligence module of the SIS records management system shall be reviewed annually by the SIS Commander for the purpose of updating or purging files which contain incorrect or obsolete information, in accordance with the Records Retention Schedule and current technological capabilities. Any information determined to be incorrect shall be immediately removed and forwarded to the SIS Commander for further action to include purging and notification of submitter, if known. Any file purge shall conform to the Records Retention Schedule.

E. An **annual review** of procedures and processes will be conducted by the Special Investigative Section Commander. Recommendations for changes shall be submitted to the Chief of Police in writing not later than March 1 of each year.

CROSS REFERENCE TO STANDARDS AND POLICIES:

CROSS REFERENCE TO FORMS: Schedule of Records Retention, Performance Evaluation Form