CRIMINAL INTELLIGENCE

EVERETT POLICE DEPARTMENT POLICY & PROCEDURE NO. **2.04**	ISSUE DATE: ___03/20/17
	EFFECTIVE DATE: ___03/20/17
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **42.1.6**	REVISION DATE: _____

I. GENERAL CONSIDERATIONS AND GUIDELINES

Intelligence is an activity principally concerned with collecting, processing, and disseminating information in specified problem areas. These areas typically include:

1. Organized criminal activities;
2. Subversive activities;
3. Vice activities;
4. Terrorism;
5. Civil disorders.

The responsibility for the department's intelligence activities may be assigned to its criminal investigation function or its vice, drug and/or organized crime control function.

This policy addresses criminal intelligence. For information on terrorism intelligence, see the department policy on ***Homeland Security***.

II. POLICY

It is the policy of this department that:

A. Intelligence gathering efforts shall not interfere with the exercise of constitutionally guaranteed rights and privileges; and

B. No intelligence information shall be gathered or retained unless it specifically relates to criminal conduct or to activities that present a threat to the community.

III. DEFINITIONS

A. *Criminal Intelligence*: Information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

B. *Intelligence:* For the purpose of this policy, intelligence refers to criminal intelligence unless otherwise noted.

C. *Reasonable Suspicion:* Information which establishes sufficient facts to give a trained law enforcement employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in criminal activity.[1]

D. *Strategic Intelligence:* Information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for both short- and long-term investigative goals.

E. *Tactical Intelligence:* Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations and provide for officer safety.

F. *Threshold for criminal intelligence:* The threshold for collecting information and producing criminal intelligence shall be the "reasonable suspicion" standard in 28 CFR, Part 23, Section 23.3 c. See "**Reasonable Suspicion**" in these definitions.

IV. PROCEDURES[2]

A. Intelligence Supervisor

1. The Chief of Police shall designate the Crime Analysis Unit who shall work with the Criminal Investigations Unit (CIU) supervisor.
   a. The CIU Supervisor and the Crime Analysis Unit shall report directly to the Chief of Police on all matters relating to the intelligence function.
   b. [S]he shall be the designated intelligence liaison for joint efforts and information exchanges with federal, state and local law enforcement agencies.
   c. It is the responsibility of the CIU Supervisor to:
      1) Ensure compliance with this policy.
      2) Evaluate raw data to determine:

a) If the data meets intelligence criteria for processing;

b) If there is any data of immediate value to the department operations;

c) If it should be processed further locally; and

d) If it should be forwarded to another intelligence-analyzing agency.

2. The Crime Analysis Unit shall monitor the data gathering, local analysis, and storage processes to ensure that all information receives appropriate disposition and that only appropriate information is retained. [S]he shall be responsible for the security of all such data.

3. The Crime Analysis Unit is responsible for disseminating intelligence information to appropriate department personnel so that investigations may be initiated when appropriate.

B. Gathering of Intelligence Information

1. GATHERING INTELLIGENCE

   a. It is the responsibility of all officers to assist in the gathering of information on organized crime, subversive activities, vice activities, terrorism and civil disorders.

   b. The department will not knowingly collect intelligence data on any individual or group merely on the basis of:

      1) The individual's or group's support of unpopular causes;

      2) The individual's or group's race, color, religion, sex, national origin, or political affiliation; or

      3) The individual's or group's lawful habits and/or predilections.

   c. Information that implicates or suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to the Chief of Police.

2. REASONABLE SUSPICION THRESHOLD: The threshold for criminal intelligence information shall be reasonable suspicion for at least one of the following criteria:

   a. Arrest, indictment, or outstanding warrant(s);

   b. Any individual identified as a perpetrator of a crime by a witness or competent evidence;

   c. Any individual who threatens violence towards persons or property;

   d. Any individual who has been or is engaged in or is conspiring to engage in criminal activity;

e. Any information that depicts the extent or scope of organized crime activity;

f. Any information relating to the identity of a victim, witness, or complainant of organized crime activity;

g. Any information relating to organized crime related social, political, business, or professional associations where said information reasonably demonstrates to the Intelligence Records supervisor that a potential for future criminal conduct exists; or

h. Any information concerning an individual's criminal activity that provides tactical and/or strategic intelligence.

3. DATA GATHERING TECHNIQUES

a. Regular conference calls and file sharing with the Boston Regional Intelligence Center.

b. Northshore Gang Taskforce Meetings, Massgangs, Coplink, Crime Analyst briefs/bulletins , other agencies bulletins, cross-dept meetings, inter-dept meetings

c. DDACTS

d. High Impact Player Meetings

e. Field Interview Cards

f. Electronic Recording Equipment

g. Surveillance Van

h. Night Vision Equipment

4. RETENTION BY INDIVIDUAL EMPLOYEES: Officers shall not retain official intelligence documentation for personal reference or other purposes but shall submit such reports and information directly to the Crime Analysis Unit.

C. Processing Intelligence Data

1. GENERALLY

a. The information gathered shall be subjected to review and analysis to derive its meaning and value.

b. Information received from outside sources shall be recorded in electronic files (emails and Sharepoint).

2. RECEIVING DATA

a. Information received from preliminary investigations or reports shall use the assigned incident numbers.

b. If a record has not received an incident number, it will be assigned one prior to being submitted to the intelligence function.

3. REVIEWING RAW DATA: The Crime Analysis Unit shall review intelligence information to ensure that the criminal data collected and maintained is limited to criminal conduct and relates to activities that present a threat to the community. [42.1.6(a)]
4. EVALUATION FOR RELIABILITY: The Crime Analysis Unit shall evaluate all sources of information to determine which of the following applies to the source: (see Coplink, CrimeIntel or Massgangs for good examples of these categories) :
    a. Completely Reliable. No question as to authenticity, trustworthiness, or competency. Information supplied by a person has proven to be reliable in all instances.
    b. Usually Reliable. There may be some doubt as to authenticity, trustworthiness, or competency. However, information previously supplied by that source has generally proven to be reliable in a majority of cases.
    c. Fairly Reliable. There may be some doubt as to authenticity, trustworthiness, or competency. However, information previously supplied by that source has generally proven to be reliable in a moderate number of cases.
    d. Unknown Reliability. Information supplied by that source cannot be determined by either judged experience or investigation. There is no way of knowing authenticity, trustworthiness, or competency.
    e. Not Usually Reliable. There is doubt as to authenticity, trustworthiness, or competency. Information previously supplied by that source has not been reliable, although occasional valid reports had been submitted.
5. All intelligence reports developed locally will indicate the source of information, including the date, from which the data were obtained. The source will be evaluated as to its accuracy and validity. Attempts should be made to substantiate the information through other sources. For information from informants, refer to the department policy on ***Use of Informants***.
6. ANALYSIS
    a. Where possible, the above-described process should be accomplished by trained professional department analysts.
    b. Data will be analyzed for local criminal intelligence value.
    c. The information shall also be forwarded to other authorized organizations for analysis, which may include:
        1) Boston Regional Intelligence Center: 617-343-4530
        2) Massachusetts Fusion Center: 978-451-3700; and

3) New England State Police Intelligence Network (NESPIN): (508) 528-8200.

4) NEMLEC

5) CJIS AND STATE RUN SITES: CRIMEINTEL, COPLINK,MASSGANGS

7. DISTRIBUTION

a. Analytic material (i.e., intelligence) shall be compiled and provided to authorized recipients as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or individuals emerge.

b. Intelligence received from other organizations will be processed through the intelligence function for distribution to affected personnel.

c. Reports and other investigative material and information received by this agency:

1) Shall remain the property of the originating agency, but may be retained by this agency.

2) Shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency.

The person disseminating intelligence information outside of the agency shall record all information disseminated in electronic files on Digital Headquarters or Outlook Email.

8. REQUESTS FOR INTELLIGENCE

a. GENERALLY: All requests for intelligence information received by the department shall be forwarded to the Records Access Officer in the Support Services Division.

b. VICE AND ORGANIZED CRIME: All requests for information concerning vice and organized crime control investigations received by the department shall be forwarded to the Special Criminal Investigations Unit (SCIU) supervisor. [S]he shall be the designated liaison for joint efforts and information exchanges with federal, state and local law enforcement agencies.

c. Where applicable, all requests for information shall be processed in accordance with the Criminal Offender Records Information Act, M.G.L. c. 6 §§168 to 178B. See department policy on ***Criminal Offender Record Information***.

D. Intelligence Records [42.1.6(b)]

1. RECORDS FILING: All record files shall include the subject's name, address and an incident number and shall be so filed as to be retrievable by any of these data fields.
2. HARD RECORD FILES: Because of the highly sensitive nature of these activities, records concerning active intelligence gathering and intelligence records shall be maintained separately from central records and central investigative records. These records shall be maintained in a secured file and shall be accessed only by the officer in charge of the investigation, the Intelligence Records supervisor, the Chief of Police, and other specifically authorized personnel.
3. ELECTRONIC FILES: Data processing systems used for these purposes shall be password-protected to limit access to authorized personnel only. Access authorization shall be controlled by the CID Supervisor.

E. Review and Evaluation of Records [42.1.6(c)]

1. All information retained shall be evaluated as to its continued relevancy and importance at least annually. The *Crime Analysis Unit* shall ensure such review.
2. The purpose of this review and audit shall be to determine:
   a. That no files are being kept which violate the substantive provisions of these procedures;
   b. That the department is following procedures which ensure that material retained is relevant to the department's mission; and
   c. That all outdated or irrelevant information is purged from the files. Such destruction shall be conducted under the direction of the CID supervisor.

F. Destruction of Records

1. All intelligence records shall be destroyed in such a manner as to make them unusable.
2. Paper records and flexible media (CDs and DVDs) shall be shredded.
3. Hard drives and other hard media shall be cleansed of data or destroyed. For further information, see the department policy on ***Computers and Data Security***.

[1] 28CFR Part 23.20(c).

[2] Recommendation 10 of the National Criminal Intelligence Sharing Plan: Law Enforcement agencies should use the IACP's Criminal Intelligence Model Policy (2003 revision) as a guide when implementing or reviewing the intelligence function in their organizations. This policy is based upon the IACP model policy.