WEBER COUNTY SHERIFF'S OFFICE

POLICY AND PROCEDURES

Intelligence Information Activities

EFFECTIVE DATE: 10/26/09 AMENDS/SUPERCEDES: 37.1; 37.3 STANDARD NUMBER: 42.1.6	REVIEW DATE: 10/26/09 REVISION DATE: 10/26/09 APPROVED: _____ Sheriff Signature

37.1.1 **Purpose**

To establish guidelines and procedures related to the gathering of sensitive but critically useful information on suspects and criminal activities.

37.1.2 **Rationale**

Criminal intelligence information gathering, analysis and the dissemination of the information are important functions in crime investigation and crime prevention. The gathering and use of such information must be done so legally and ethically. The activities related to intelligence information gathering must be carefully carried out with respect to legal restraints, individual privacy and deputy safety.

37.1.3 **Definitions**

Criminal Intelligence Information: data which has been evaluated to determine that it is relevant to the identification of, and the criminal activity engaged in, by an individual who, or organization which, is reasonably suspected of involvement in criminal activity or conduct. Examples of criminal activity may include but are not limited to:

1. Domestic and international terrorist groups,
2. Potential terrorism related activities,
3. Robbery and burglary rings,
4. Organized criminal cartels,
5. Vice, drugs and organized crime activities,
6. Criminal street gangs,
7. Criminal motorcycle gangs,
8. Sexual offenders.

37.1.4 **Policy**

It is the policy of this office to establish procedures for handling intelligence information in a manner that is both conducive to the investigation and prevents criminal conduct while protecting the rights of individuals.

37.1.5 **Procedure**

A. Responsibilities of all employees

1. The collection of criminal intelligence about individuals, groups or enterprises is limited to criminal conduct and will relate to activities that present a threat to the community.

    a. Information may be collected and maintained under the following guidelines:

        i. If evidence exists connecting persons with known or suspected criminal activity; and,
        ii. The information is relevant to the criminal activity.

    b. Information will not be collected or maintained by Sheriff's Office solely on a person's:

        i. Support of unpopular cause,
        ii. Race or ethnicity; or
        iii. Religious and/or political affiliations.

2. Employees will not knowingly engage in illegal activity in the collection of intelligence data, nor shall they direct any other person to engage in the collection of intelligence data through illegal means.

3. Dissemination of criminal intelligence information is the responsibility of the Intelligence Investigator.

4. Supervisors will routinely inspect collected intelligence information to ensure that it meets the requirements of this chapter.

5. At least annually, a supervisor or Sheriff's designee will review all intelligence gathering procedures and processes for continued application and report the review findings to the Sheriff.

B. Training:

1. The division will be staffed with trained personnel capable of conducting effective crime analysis and intelligence gathering and dissemination techniques. This training will be received through either formal classroom, routine staff meetings, and/or on-the-job training conducted by the Division Commander or his designee.

C. Storing of Information/Intelligence

1. All intelligence information received will be stored in an intelligence file.

2. The intelligence file can be either electronic or paper.

3. The manner of storage must provide for limited access.

    i. If stored electronically, the information must be stored in a secure format-i.e. password protected-which limits access.
    ii. If hard copies (paper) are stored, they must be stored in a locked cabinet to which the access is limited.

D. Documentation, Reporting of Information

1. The receipt of intelligence information is to be documented and shall include (if available):

    i. The date the information was received.
    ii. The identity of the person providing the information.
    iii. The identity of the Deputy forwarding the information.
    iv. A description of the information received.

2. If information is shared with any individuals or groups, a record must be kept of:

    i. The date the information is released.
    ii. The name of the person or persons receiving the information.
    iii. A description of the specific information released.

3. If additional investigation is needed, the Investigator will assess the usefulness of the information by considering the following:

    i. Reliability of the person providing the information. Factors to consider are: Willingness to provide his/her name,

address, etc. Willingness to testify. Accuracy of information provided in the past.

ii. Whether or not the information can be corroborated by other sources.

iii. The amount of information provided.

4. If the Intelligence Investigator believes there exists sufficient information, he/she will generate a formal case by obtaining a case number through dispatch.

E. Sharing/Dissemination of information.

1. It is the responsibility of this Office to provide relevant intelligence information to those individuals or agencies responsible for conducting an investigation.

2. Requests for intelligence information, whether made from inside or outside this Office, shall be directed to the appropriate Intelligence Investigator.

3. Prior to releasing the information the person receiving the request:

i. Must determine if the person submitting the request has a legitimate need to know the information being requested.

ii. May ask for clarification in order to help determine the appropriate information to release.

iii. Determine if releasing the information will put the source of the information at risk.

4. Information shall not be released to non-law enforcement individuals or agencies.

F. Purging of Intelligence Records.

1. Intelligence files shall be reviewed periodically to insure that they do not contain out-of-date or incorrect information. Such information shall either be corrected or purged.

i. Files cannot be purged without the approval of an Investigations Supervisor.

ii. Paper files to be purged shall be shredded.

iii. Electronic files to be purged shall be deleted.