WEBER COUNTY SHERIFF'S OFFICE

POLICY AND PROCEDURES

Safeguarding and Security of Intelligence Information

EFFECTIVE DATE: 10/07/03 AMENDS/SUPERCEDES: 37.3 STANDARD NUMBER: 51.1.2	REVIEW DATE: 07/15/05 REVISION DATE: 07/15/05 APPROVED: _____ Sheriff Signature

37.3.1 **Purpose**

To safeguard intelligence information and protect it against unauthorized or improper use.

37.3.2 **Rationale**

Criminal intelligence information can be highly sensitive. Its authorized, legal and proper use can aid in crime detection, intervention and enhance overall public safety efforts. The unauthorized use of this information can compromise deputy safety and criminal prosecutions and increase civil liability. Controlling who has access to this information, and specifying how this information is to be used, resolves these issues.

37.3.3 **Policy**

A. The Office will safeguard intelligence information and secure intelligence records separate from all other records.

B. Only authorized personnel will have access to criminal intelligence records. Authorized personnel include:

1. the Sheriff,
2. the Professional Standards Bureau Commander,
3. the Internal Affairs Unit Supervisor, and
4. others as designated.

37.3.4 **Procedure**

A. Intelligence files will be:

1. Decentralized from other agency records,
2. Separately maintained and secured in a locked file cabinet by the Professional Standards Bureau Captain or designee; and/or in the Versaterm records system with access restricted by the "privatized" function of the Versaterm system,

3. Separately identified in the Versaterm records system offense codes as "Public Peace-Intelligence Cases",

4. Restricted to access by the Professional Standards Bureau Captain or his/her designee or the Internal Affairs Unit Inspector Sergeant,

5. Tracked using Dispatch issued Intelligence case numbers which shall be recorded on the Versaterm records system by the investigator.

6. Documented either using the Versaterm records system case report format and stored in the system; and/or when appropriate, intelligence documents may be stored in files identified with the Intelligence case number and stored in locked Professional Standards Bureau Intelligence files.

B. Intelligence information received should be:

1. Assessed and filed according to the following categories:

   a. Outlaw motorcycle gangs
   b. Street gangs
   c. Criminal suspects/organizations
   d. Probation and Parole (periodic interagency bulletin, PIB)
   e. Sex Offenders (PIB)
   f. SHOCAP Bulletins (PIB)
   g. RMIN Bulletins (PIB)
   h. Field Interviews of special interest
   i. Public Safety Alerts (PIB)
   j. Vice, Drugs, Organized Crime

2. Except in case of periodic bulletins, assigned an Intelligence Case number:

   a. By the Professional Standards Section Lieutenant or designee, or Section Inspector Sergeant.

b. If reasonable suspicion of criminal activity or conduct is present,
c. Using the appropriate Versaterm offense code designation.

3. Evaluated regarding reliability (WCSO P&P 29.17.1C)

a. High Reliability
b. Usually Reliable
c. Not Often Reliable
d. Reliability Unknown

4. Documented

a. Assigned Intelligence Case number
b. Date, Time received
c. Date, Time reviewed/purged
d. Source
e. Type/category
f. Reliability Factor
g. Summary
h. Action Taken (file only, forwarded, active investigation)
i. Dissemination date, reason, person or organization

5. Disseminated

a. To appropriate Bureau, Section, Personnel
b. To appropriate outside agency
c. To File
d. Requests will be in writing on appropriate letterhead or Office form
e. Requesting party will provide reason, authorization for request, and specific information requested,
f. Person disseminating information will document the reason, date, time, person and/or organization being given the information.
g. Documents disseminated should be stamped as “confidential”

6. Schedule of Records Review/Purging

a. Periodic bulletins - monthly
b. Field Interviews - monthly
c. Gangs - annually
d. Public Safety Alerts - monthly
e. Vice, drugs, organized crime - annually
f. Criminal suspects/organizations - annually

7. Purging

    a. Review of record/file by Professional Standards Bureau Captain or designee.
    b. Identification of intelligence information to be purged.
    c. Delete intelligence information from Versaterm record system.
    d. Document date, time, and the person doing the purging of the information, in narrative section of record.

e. Documents secured in Section office files may be shredded or submitted to the Office Evidence Custodian to be burned, and notation made on Versaterm record.
f. Periodic interagency bulletins (PIB) are not assigned an intelligence case number and documentation of purging is not required,

C. Dissemination Verification

1. Will be the responsibility of the Professional Standards Bureau Captain or designee to:

a. determine that recipients of disseminated intelligence information have not misrepresented themselves, and
b. are authorized to make the request or receive the information, and
c. have a "need to know," and
d. that all disseminations are accomplished in a manner which reflects state and federal laws.

2. The Professional Standards Bureau Captain or designee will:

a. coordinate with the Investigations Section Lieutenant and the Patrol Operations Bureau Commander regarding intelligence information received and/or disseminated to or from respective Section or Bureau personnel or other agencies.

b. coordinate intelligence gathering activities related to collection, general assessment and storage of intelligence information.

3. Will be established by:

a. Credentials.
b. Return phone numbers.
c. Requests on official letterhead.

D. Information Processing

1. will be conducted in an environment protected from inadvertent disclosure of information,

2. Will normally be conducted in the secured Offices of the Professional Standards Section

E. Computer based systems used to process and/or store intelligence information, if applicable, will:

1. Incorporate the Versaterm “privatized” function to ensure user identifier codes and write protect procedures are applied, to secure information from unauthorized access, modification, removal, and/or destruction.

2. If restricted by Federal Government grant agreements, specifically IBM notebooks, Toshiba and Panasonic laptops, WILL NOT be used for storage of criminal intelligence information.