WEBER COUNTY SHERIFF'S OFFICE

POLICY AND PROCEDURES

COMPUTERIZED SECURITY PROTOCOL

EFFECTIVE DATE: 07/30/09 AMENDS/SUPERCEDES: See attached sheet STANDARD NUMBER: 82.1.7	REVIEW DATE: 07/30/09 REVISION DATE: 07/30/09 APPROVED: _____ Sheriff Signature

54.9.1 Purpose

To establish a security protocol for access and release of computerized records.

54.9.2 Rationale

To ensure that the Weber County Sheriff's Office is following all guidelines set forth by BCI Standards for access to BCI controlled records. Also that the Support Services Division maintains proper confidentiality, as set by GRAMA requirements, when releasing records to the public and other criminal justice agencies.

54.9.3 Policy

A. Computerized Criminal History Access by Sheriff's Office personnel is controlled and managed by the Support Services Division Manager or Designee who:

1. Assigns and authorizes all Office computerized criminal history and records access.

2. Determines levels of access by assignment and need to know.

3. Restricts access to sworn deputies and Support Services Division office staff.

4. Assigns security and access levels by group and/or individual.

5. Assigns a specific "user name" and "password" for each user.

6. Revokes access depending on assignment and need to know.

7. Conducts on going review of employee termination or resignation or change of assignment in order to revoke or re-assign user name, passwords and access levels.

8. Conducts an annual audit of users for the purpose of assignment or revocation of user names, passwords and access levels.

B. Release of Criminal Description records from Versaterm to the public are determined by the Government Records Access and Management Act (GRAMA) regulations and Office Policy.

C. Release of Office records to other bonafide Criminal Justice Agencies may be made by Deputies or Office Staff with the approval of the Support Services Division Manager or Designee. Records released must be stamped with the Appropriate confidentiality classification per the Government Records Access and Management Act (GRAMA) requirements, and must be treated as such.

D. Criminal History records, specifically Utah BCI and NCIC III, may be accessed by authorized Office personnel for Office use only. Such records WILL NOT be released to any other law enforcement agencies or private individuals, businesses or groups.

E. Information stored in all UCJIS files is confidential and must be protected to ensure legal dissemination. Unauthorized request or receipt of this information could result in criminal proceedings. Violation of privacy and security regulations can also result in criminal prosecution of the person(s) involved and loss of state computer access by this agency. There is also potential for civil actions as well.

Each user is required to sign and date a BCI security statement and agreement at the time of certification/recertification.

Any user that is thought to be accessing the UCJIS system unlawfully or for reasons other than allowed by UCJIS/Weber County Sheriff's Office policies will be immediately removed from access into the UCJIS system while the incident is investigated. The investigation will be handled by the TAC and/or the IA officer for WCSO. The investigation will adhere to the policy of BCI, including using a BCI Dissemination Log Form if required. It is required that we notify BCI in the event of misuse of the UCJIS files. The disciplinary action will be decided through their chain of command, and may involve loss of access, re-assignment, up to and including termination.