WEBER COUNTY SHERIFF'S OFFICE	POLICY AND PROCEDURES
SUBJECT: Mobile Computer Access, Security Procedures	CHAPTER/SECTION NO.: 28.39
EFFECTIVE DATE:	REVIEW DATE:
AMENDS/SUPERSEDES: See attached sheet	APPROVED: ***** See Master File*** **Sheriff**
STANDARD NUMBER: 41.3.7	

28.39 **Policy**

28.39.1 All computer equipment owned by the County and used by Sheriff's Office shall be operated to comply with the State of Utah Bureau of Criminal Identification Information Resources Acceptable Use Policy per section 53-10 Utah Code Annotated; and any applicable Weber County Sheriff's Office policies.

28.39.2 **PROCEDURE**

A. Inventory and Location of Equipment

1. All mobile data computers shall be inventoried by designated Sheriff's Office personnel. An inventory tracking log shall be kept on the equipment and will be used to show the current status and location of each piece of equipment. All applicable information on the log shall be filled in by the issuing supervisor for each piece of equipment and initialed y portions of the log and initial receipt of the equipment placed back into storage.

B. Physical Security

1. Mobile computers shall be removed from the vehicle and placed in an area

protected from excessive climatic extremes when the vehicle is unoccupied for extended periods of time. Mobile computers which must be left in vehicles during extremely hot conditions shall be covered with a protective cloth.

2. Information obtained from BCI and NCIC are considered privileged and care must be taken to safeguard access. The computer should be positioned to prevent casual access to the information on the screen. During break or other periods of inactivity, the computer should have the screen closed.

C. Information Security

1. Information obtained from BCI (driver license information), registration information, criminal history, NCIC and statewide warrants) is considered confidential and protected. This information shall be used in the performance of police-related activities and any other use is forbidden and subject not only to departmental sanction, but possible civil and criminal penalties. Information from these sources will not be obtained for any other purpose. Such information may not be released to anyone outside of police channels or for purposes other than bonafide investigations. Release of such information can result in civil penalties for the operator as well as termination of employment. Passwords shall not be given out to others, even those with the same or greater access rights to the system. Operators are encouraged to change passwords frequently and in a random manner to avoid detection of passwords by others. It is mandatory that all passwords be changed every forty-five (45) days.

Passwords are not to be given out to others, even those who have the same or greater access rights to the system. Operators are required to log off the various systems when leaving the computer terminals unattended in unlocked areas.

D. Software Ownership and Security

1. Only County approved software may be installed on County issued computer. All software installations will be performed by sheriff's office computer services technicians or Weber County Information Technology personnel. Software purchased by the County is for installation and use only on the County owned computers for which it is licensed. County owned software may not be installed or used on private computers or other County owned computers without proper license and authorization.

E. Data and Virus Protection

1. Each computer will be periodically scanned for viruses by Information Technology using programs approved and purchased by the County. Removable media (floppy disks, tapes, etc.) obtained from outside sources will <u>not</u> be installed or used in the computers without prior approval from the Sheriff's Office. Removal of detected viruses can damage other information stored on the computer and therefore viruses should not be removed by anyone other than Information Technology personnel.

F. Unauthorized Software Installation

1. No unauthorized, unlicenced or

unsuitable material shall be installed. The computer will be periodically monitored by Sheriff's Office MIS or County Information Technology or a supervisor for the presence of unlicenced software or other unauthorized material. The presence of pornographic or other similar material may be grounds for disciplinary action.

G. Personal Conduct

1. The computer shall not be used to distribute offensive or harassing statements, or to disparage others based on race, national origin, sex, sexual orientation, age, disability or political or religious beliefs. For the protection of the Office and members, an ongoing audit process will be conducted as all entries into any department computer system, including messaging and e-mail, may become legal documents and as such are subject to being subpoenaed. Inappropriate conduct will result in disciplinary action up to and including termination.

H. Equipment Maintenance and Care

1. Defects in the computer hardware and software systems should be documented and reported to the appropriate supervisor as soon as they are noticed. If a member experiences a problem with the unit, the deputy will check the unit back in to a designated supervisor. The member experiencing the problem will write a brief description of the problem and this will be left with the mobile computer. Maintenance may only be performed by those authorized by Information Technology.

2. The computer is to be kept free from

dust, moisture, excessive heat and other damaging conditions. The screen should be cleaned with a soft cloth and a cleaner specifically recommended for computer screens. Keyboards and CPU cases should be cleaned with an appropriate cleaner. Abrasives should never be used. For cleaning needs other then basic maintenance contact the Sheriff's Office Management Integrated Systems (MIS) technicians.

3. All systems will be protected by an electric surge protector installed in the vehicle by Weber County Fleet Management.

I. Safety

1. Computers may not be used to obtain information while the vehicle is in transit, unless a second authorized deputy is in the vehicle and conducting the inquiry. If it is urgent that you obtain the information while in transit, you must immediately switch to verbal communication through the dispatch center. If a deputy receives a possible hit on an NCIC entry, i.e. wanted or missing person, stole vehicle, stole gun, you must switch to verbal communication through the dispatch center.

J. System Authorization and Password Requests

1. Requests for access authorization and passwords to the various systems within the system will be approved by the division commander.

K. Private Use of County Owned Equipment

1. Employees may not use County owned computer equipment for private purposes.