Kern County Sheriff's Office

Policies and Procedures

TITLE: **USE OF COMPUTER SYSTEMS AND DATA**			NO: J-1610
APPROVED: **Donny Youngblood, Sheriff-Coroner**			
EFFECTIVE: **February 1, 1996**	**REVIEWED:** 06/08/2018	**REVISED:** 07/20/2015	**UPDATED:** 06/08/2018

POLICY

The Kern County Sheriff's Office recognizes that access, use, and maintenance of confidential data contained in law enforcement related databases and computer systems are essential to meet various law enforcement needs.

The rapid expansion and proliferation of computer systems containing confidential data increases the responsibilities of all personnel who have the authorization and ability to view or access those systems. Misuse of the systems or data adversely affects the civil rights of the individuals concerned and violates the law.

It is the responsibility of all personnel who access, use, or maintain this data to do so in accordance with the law. Any unauthorized or misuse of those systems or data will not be tolerated.

Any employee who is responsible for such misuse is subject to disciplinary action including suspension, dismissal, or other disciplinary action. Violations of the law may also result in criminal and/or civil action.

In addition to administrative action, criminal prosecution or other civil remedies available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under Penal Code Section 502 for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access.

DEFINITIONS:

PERSONNEL: All members of the Sheriff's Office whether officers or employees, sworn or non-sworn, permanent, part-time, extra help, volunteer, or under contract.

DATA: A representation of ALL information, knowledge, facts, concepts, computer software, computer programs or instructions which includes, but is not limited to data maintained in NCIC, CLETS, CJIS, CAD, INMATE MANAGEMENT, CAL GANG, IAPRO, PAROLE LEADS, COPLINK, SMART JUSTICE, CAL PHOTO and IDENTIX systems.

RIGHT TO KNOW: The right to obtain data from any law enforcement computer network, computer software, computer program, computer service or computer system, pursuant to court order, statute, or law.

NEED TO KNOW: A compelling need is established when the Sheriff's Office or individual employee needs the information in the course of their official authorized duties and there is no other practical way that they can obtain it.

ACCESS:

DIRECTIVE A

Only those persons authorized by nature of their duties and having a right and need to know shall access or be allowed to access any law enforcement computer systems or manual databases.

DIRECTIVE B

All personnel shall, upon completion of needed access to any law enforcement computer system, immediately sign off from the system and not leave the system unattended.

DIRECTIVE C

All personnel shall maintain confidentiality of their password and not share or divulge the password to other employees.

DIRECTIVE D

All employees shall restrict the use of their password to their own authorized use.

CONFIDENTIALITY:

DIRECTIVE A

Information contained in the various law enforcement related databases and computer systems are considered to be confidential and shall only be used in the scope of the employee's official authorized duties.

DIRECTIVE B

Employees shall not access, use, or maintain any computer databases or manual records for other than official authorized legitimate law enforcement purposes.

DIRECTIVE C

Persons who access and misuse the various systems or data risk disciplinary action up to and including dismissal, criminal prosecution, and civil liability. Penal Code 502 contains subsections defining computer crimes as either a misdemeanor or felony. For instance, a violation may be punishable by a fine not exceeding $10,000 or by imprisonment in the state for up to 3 years or both fine and imprisonment.

DIRECTIVE D

Personnel who witness or have knowledge of the misuse of any law enforcement computer system, database, or manual records shall report the misuse to their immediate supervisor.

EFFECTIVE:	**REVIEWED:**	**REVISED:**	**UPDATED:**
February 1, 1996	06/08/2018	07/20/2015	06/08/2018

TRAINING:

DIRECTIVE A

No employee will be granted access to any law enforcement related databases or computer systems without first receiving prior training. Training will only be conducted by authorized personnel as designated by the Sheriff's Office CLETS and CJIS coordinators in conjunction with the Training Section.

DIRECTIVE B

No employee will be granted access to the CLETS, CJIS, INMATE MANAGEMENT, CAL GANG, IAPRO, COPLINK, OR SMART JUSTICE systems until they have successfully completed a record or background check and have it on file in the Training Section.

DIRECTIVE C

The Sheriff's Office CLETS and CJIS coordinators will be responsible for entry and deletion of employee's access into the various systems covered under this procedure.

DIRECTIVE D

Following the established training each employee will read and sign an **Employee Statement Form** acknowledging that they are familiar with the policies, laws and regulations concerning the access, use, and maintenance of confidential data contained in the various law enforcement related data bases and computer systems. (See Exhibit A).

DIRECTIVE E

The original or electronically signed copy of the **Employee Statement Form** will be maintained in the employee's personnel file.