CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (CLETS)

AUTHORITY: Administrative Directive

RESCINDS: Procedural Manual Item 1-4-208, dated 10/20/19

FORMS: CLETS Employee/Volunteer Statement
CLETS Management Control Agreement
CLETS Private Contractor Management Control Agreement
FBI CJIS Security Addendum

PURPOSE: To describe the criteria for accessing, safeguarding, and misuse of CLETS and its information/database.

I. GENERAL INFORMATION

A. California Law Enforcement Telecommunications System (CLETS) is a communications network available to all public agencies of law enforcement within the state. CLETS provide**s** all law enforcement and criminal justice user agencies with the capability of obtaining information directly from federal and state computerized information files.

B. Each CLETS subscribing agency must designate an Agency CLETS Coordinator (ACC) who serves as the point of contact with California Department of Justice (CA DOJ) on matters pertaining to the use of CLETS, Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (NLETS), and CA DOJ criminal justice databases and administrative network CLETS accesses. The ACC will be responsible for ensuring compliance with CA DOJ/FBI policies and regulations, including validation requirements, as well as facilitate the exchange of CLETS administrative information between CA DOJ and ACC's agency. The Office Manager at Manchester Office Building (MOB) is Orange County Probation Department's (OCPD) designated ACC.

C. Each CLETS subscribing agency must designate a Local Agency Security Officer, hereinafter referred to as the Security Point of Contact (SPOC), who serves as security coordinator with CA DOJ on security matters pertaining to the use of CLETS, NCIC, NLETS, and CA DOJ criminal justice databases and administrative network CLETS accesses. Any information communicated between CA DOJ and SPOC will be shared with the Agency's ACC. Orange County Information Technology (OCIT) Cybersecurity Operations Manager is designated as the SPOC.

D. A County Control Agency (CCA) will be designated in each county to coordinate the connection of law enforcement and criminal justice agencies to CLETS. The Sheriff's Office will serve as CCA, unless CA DOJ, in consultation with the CLETS Advisory Committee (CAC), indicates another law enforcement agency in the county is better qualified.

The CCA is responsible for providing CLETS service via its Message Switching Computer (MSC) to all qualified CLETS subscribing agencies within their respective county.

II. PROCEDURE

A. Confidentiality of Information from CLET

Only authorized law enforcement, criminal justice personnel, or their lawfully authorized designees may use a CLETS terminal. Any information from CLETS is confidential and for official use only. Access is defined as the ability to hear or view any information provided through CLETS.

Each employee, volunteer, and private contractor is required to sign an Employee/Volunteer Statement prior to operating or having access to CLETS terminals, equipment, or information. This form addresses confidentiality, release, and misuse of information from CLETS.

1. Information from CLETS is on a “right-to-know” and “need-to-know” basis.

2. Authorized personnel shall not inquire into their own record or have someone inquire for them.

3. Accessing and/or releasing information from CLETS for non-law enforcement purposes is prohibited, unless otherwise mandated, and is subject to administrative action and/or criminal prosecution.

4. All investigation of misuse must be reported to CA DOJ on CLETS Misuse Investigation Reporting form, including investigations where misuse was not found. The **Facilities and Safety Manager**, is responsible for reporting misuse annually **to the PSD Division Director**.

B. CLETS Access Requirements

1. CLETS access is permitted only from an agency device or terminal licensed and approved by DOJ. Reasonable measures shall be taken to place terminals and equipment in an area with adequate physical security to provide protection from vandalism or sabotage and to preclude public view. This includes unauthorized viewing or access to computer terminals, access devices, or stored/printed data at all times.

2. All persons, including non-criminal justice, volunteer personnel, and private vendor technical or maintenance personnel, who have physical access to CLETS equipment, information from CLETS, or to Criminal Offender Record Information (CORI) are required to undergo a background and fingerprint-based CORI search. Pursuant to FBI’s CJIS Security Policy section 5.12, if the fingerprint-based CORI search reveals a felony conviction of any kind, CLETS/NCIC access shall not be granted. If it is revealed the person has an arrest history without conviction for a felony, the agency head or his/her designee will review the matter and decide if CLETS access is appropriate.

C. CLETS Users Defined

1. Full Access Operators (FAO)

Any operator who has a CLETS User ID and password, makes inquiries into the systems, and/or performs update functions.

a. Within six (6) months of appointment, the FAO must be trained in the operations, policies, and regulations and must complete the appropriate CLETS/NCIC Telecommunications Proficiency Examination approved by CA DOJ.

b. Biennially (every other year), the FAO must complete a current FAO Proficiency Exam (with a passing score of at least 70%) and the Employee/Volunteer Statement.

c. Annual completion of a Department of Motor Vehicles (DMV) confidentiality statement is also required.

2. Less Than Full Access Operators (LTFAO)

Any operator who has a CLETS User ID and password, and makes inquiries into the systems. LTFAOs do not perform update functions.

a. Within six (6) months of appointment, a LTFAO must be trained in the operations, policies, and regulations and must complete the appropriate CLETS/NCIC Telecommunications Proficiency Examination approved by CA DOJ.

b. Biennially (every other year), a LTFAO must complete a current LTFAO Proficiency Exam (with a passing score of at least 70%) and the Employee/Volunteer Statement.

c. Annual completion of a DMV confidentiality statement is also required.

3. Practitioners

Any person who has access to information from CLETS, and is not a CLETS operator. Access to information may be intended or accidental.

a. Within six (6) months of appointment, practitioner personnel must receive basic training in CLETS/NCIC policies, liability issues, and regulations. For example, non-criminal justice, volunteers, and private vendor technical or maintenance personnel.

b. All Practitioners must complete the Security Awareness training and test.

4. Administrators

Any person designated criminal justice administrators and upper-level managers.

a. Provided peer-level training on CLETS/NCIC system use, regulations, policies, audits, sanctions, and related civil liability. Training is accomplished by reviewing and signing for the NCIC “Areas of Liability for the Criminal Justice Information System Administrator” packet.

b. Administrators must complete the Security Awareness training and test.

D. CLETS Certification Testing/Training

The ACC will ensure all persons with access have competed CLETS training and testing as required by CA DOJ.

1. Within six (6) months of employment or assignment, all sworn/non-sworn practitioner personnel must receive basic training in CLETS/NCIC policies, liability issues, and regulations.

2. Security and awareness training shall be required for all personnel who have access to CLETS systems and shall meet the requirements specified within FBI CSP section 5.2.

E. CLETS Sanctions for Misuse

1. As a member of OCPD, you may have access to confidential criminal record and/or DMV record information, which is controlled by statute. Misuse of such information may adversely affect an individual's civil rights and violates the law.

2. Misuse is defined as CLETS information obtained or provided outside the course of official business; a "right to know" and the "need to know" must be established.

a. The "right to know" is defined as "authorized access to such records by statute.

b. The "need to know" is defined as "the information is required for the performance of official duties or functions.”

c. Other than blatant misuse, the following are examples of prohibited/unauthorized use of CLETS by federal, state, or local law enforcement agencies that include, but are not limited to:

(1) Querying yourself, a family member, friend, etc.

(2) Providing information from CLETS to another officer, individual, agency, or company for unauthorized purposes

(3) Sharing user IDs or passwords

(4) Logging into CLETS and allowing others to utilize your authorized access

(5) Querying the Automated Criminal History System for licensing, employment, or certification purposes (e.g., Carry Concealed Weapon permits)

(6) Querying a firearm to determine if it is stolen prior to purchase

(7) Querying the DMV to obtain unauthorized address, vehicle registration, or insurance information (e.g., querying a vehicle parked in front of your house for two days)

(8) Querying high profile individuals in the media

(9) Using any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. § 1373 and § 1644.

3. PSD shall investigate incidents of system misuse by reviewing its internal processes, documentation, and the DOJ Policies, Practices and Procedures for authorized usage.

a. Violations can result in administrative discipline, up to and including discharge.

b. Violations of this law may also result in criminal and/or civil actions.

REFERENCES:

Procedures:	1-4-207	Physical Protection of Criminal Justice Information
	1-5-306	Media Sanitization/ Destruction and Protection
Policy:	B-1	Case Confidentiality – Client's Right to Privacy
	B-2	Inter- and Intra-Agency Confidentiality
	B-3	Case File Management and Security
	C-18	Investigations: Departmental Response to Allegations of Employee Misconduct
	G-12	Personally Owned Electronic Devices
	G-13	Electronic Information Devices
	G-15	County's Information Technology Usage Policy

CLETS Policies, Practices and Procedures (and Statutes)
FBI CJIS Security Policy

V. Sanchez

APPROVED BY: Dana Schultz Digitally signed by Dana Schultz Date: 2022.02.09 09:13:55 -08'00'