240-547-5446
info@gkaccess.com
gkaccess.com

CLETS Compliance - GateKeeper

Why CLETS Compliance Matters

The California Law Enforcement Telecommunications System (CLETS) is a critical database used approximately **2.8 million times per day** by law enforcement to access sensitive information—ranging from driver's licenses and vehicle registrations to criminal histories and restraining orders. Access is strictly limited to authorized criminal justice personnel, such as dispatchers, sworn officers, investigators, records clerks, and supervisors, all of whom must undergo background checks, fingerprinting, and training.

Because CLETS contains Criminal Justice Information (CJI), it is subject to **strict authentication, session control, and audit requirements** set by the California DOJ. Agencies must enforce "right-to-know" and "need-to-know" access policies, conduct annual misuse reporting, and comply with both **physical security controls** and **information security protocols**.

Misuse, such as querying family members, public figures, or using data for personal reasons, is a violation of California law, with potential consequences including disciplinary action, termination, legal penalties, and even criminal charges. Despite mandatory reporting requirements, historical compliance rates have been low, and even confirmed violations often result in minimal discipline. This gap between policy and consistent accountability makes strong access controls and auditable systems even more vital.

Key CLETS Security Dimensions

CLETS (California Law Enforcement Telecommunications System) access and usage must adhere to strict security requirements to protect sensitive criminal justice data and ensure operational integrity. The key security dimensions include:

- **Controlled Access:** Terminals for official law enforcement use only; operate in supervised, secure areas; turn off when unsupervised.
- **Passwords:** Min. 8 characters, no dictionary words/names, not the same as user ID; change every 90 days; no reuse of last 10; never post, write, or share; remove compromised/unneeded passwords immediately.
- **Data Protection:** Maintain confidentiality, integrity, and availability; prevent unauthorized access or viewing of criminal justice data.
- **User Practices:** Lock/log off unattended terminals; remove access when no longer needed.

Key CLETS Requirements and How GateKeeper Delivers Compliance

GATEKEEPER

240-547-5446
info@gkaccess.com
gkaccess.com

GateKeeper, a proximity-based multi-factor authentication (MFA) solution, directly addresses multiple CLETS security requirements while improving workflow efficiency for officers and dispatchers.

CLETS Section	CLETS Requirement	How GateKeeper Meets It
1.6.1 – Unique User ID	All system users must have a unique identifier.	Each officer is issued a dedicated proximity token + PIN, eliminating shared logins.
1.6.2 – Authentication	All users must authenticate before accessing CJI.	MFA with proximity token + PIN before any CLETS access.
1.7.1 – Automatic Logoff	Workstations must log off after max 30 minutes of inactivity.	Proximity-based lock triggers instantly when the user walks away.
1.7.2 – Unattended Terminals	Terminals must lock when unattended.	Auto-locks within seconds of departure, preventing "walk-away" exposure.
5.5.1 – Physical Security	CLETS terminals must be physically secured.	Adds an electronic authentication barrier beyond physical security measures.
7.3.1 – Audit Records	The system must log all user access to CJI.	Records every login, logout, and lock/unlock event tied to specific users.
7.3.2 – Shared Devices	Agencies must identify each user on shared devices.	Fast user switching with unique tokens; no password sharing.
8.2.1 – Policy Enforcement	Agencies must enforce authentication & access control policies.	Automatically enforces MFA, lock rules, and unique logins every time.

How GateKeeper Strengthens CLETS Compliance

- **Enforces DOJ Password & Access Policies**
  - Meets the DOJ's strong password requirements while reducing reliance on manual password entry.
  - Eliminates password sharing through unique proximity tokens.
- **Prevents Unauthorized Access**
  - Proximity-based session locking stops access the moment a user steps away, addressing unattended terminal risks.

240-547-5446
info@gkaccess.com
gkaccess.com

- **Supports Audit & Inspection Readiness**
  - Generates complete audit trails of user-specific activity, simplifying periodic DOJ/FBI inspections and annual CLETS misuse reporting.
- **Enhances Physical and Digital Security**
  - Combines electronic access control with proximity authentication for CLETS terminals, fulfilling both physical security and logical access requirements.
- **Maintains Workflow Efficiency**
  - Officers and dispatchers can log in and out in seconds, enabling compliance without slowing field operations or dispatch responsiveness.

Benefits for CLETS Agencies

- **CJIS-Aligned MFA**: Meets state and federal standards without adding friction for officers.
- **Zero Password Sharing**: Improves accountability, especially on shared MDTs and workstations.
- **Instant Session Lock**: Prevents unauthorized access in real time.
- **Operational Efficiency**: Enables fast, secure access during time-sensitive law enforcement activities.
- **Complete Audit Trails**: Simplifies compliance reviews with precise user logs.