CLETS (California Law Enforcement Telecommunications System): Incident Response Plan

303.1 PURPOSE:

To provide a process for reporting: misuse, abuse, suspected data compromise and stolen CLETS equipment. While establishing guidelines to standardize the operating practices of CLETS and the rules and ramifications set forth by the California Department of Justice (DOJ) relating to the confidentiality and operations of CLETS.

303.2 DEFINITIONS:

California Law Enforcement Telecommunications System (CLETS): Provides vital information to Law Enforcement agencies. The system's network is an interlink of the following agencies: National Crime Information Center (NCIC), Criminal Justice Information System (CJIS), National Law Enforcement Telecommunications System (NLETS), California Department of Motor Vehicles (DMV), and Oregon's Law Enforcement Data System (LEDS).

Department of Justice (DOJ): California Law Enforcement Regulatory Agency. DOJ controls CLETS usage statewide.

Subscriber: The Head of the Department and Chief Administrator of CLETS operations.

CJIS Systems Agency Information Security Officer (CSA ISO): Serve as the security point of contact (POC) to the FBI CJIS Division ISO. Documents technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA user community, to include the local level. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, of the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJIS.

Terminal Agency Coordinator (TAC): The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

CLETS Trainers: Employees designated by the appointing authority to provide CLETS training to personnel. Trainers must be certified through the DOJ.

Administrators: Deputy Chiefs, Director I/IIs and Administrative Managers.

Right to Know: The right to obtain criminal offender record information pursuant to court order, statute or decisional law.

Need to Know: The necessity to obtain criminal offender record information in order to execute official responsibilities.

Criminal Offender Record Information (CORI): The summary information relating to arrests, pretrial proceedings, sentencing information, incarcerations, parole and probation (PC11075).

Criminal Justice Information Services (CJIS): A compilation of data, fingerprints, reports and records from law enforcement detailing the state of crime in communities across the country, made available to authorized local, state, federal and international law enforcement agencies.

CJIS Systems Agencies (CSA): Responsible for establishing and administering an information technology security program throughout the CSA's user community, to include local levels.

CJIS Systems Officer (CSO): The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

303.3 GUIDELINES:

A. All employees of the Department shall comply with state and local regulations regarding the use of CLETS and required to take security training.

B. It is the responsibility of all agencies covered under this policy/procedure to ensure the protection of criminal justice information between the Federal Bureau of Investigations (FBI) CJIS division and its user community.

C. Periodic driver license checks may be conducted via CLETS on the employees of the subscribing agency when driving is a requirement of the employee's job.

D. Only authorized personnel should be performing interviews or examining evidence. The authorized personnel may vary by situation.

E. Violations of the Penal Code, CLETS rules, regulations, policies, and procedures may result in the following sanctions: Removal of CLETS service, Personal punitive damages paid by sworn or non-sworn employee or Department, Disciplinary actions at the Department level, Referral to external Law Enforcement for prosecution.

F. Any information accessed through CLETS is confidential.

G. Access is defined as the ability to view any information provided through CLETS or the ability to hear any information provided through CLETS.

H. Only authorized law enforcement personnel or their lawfully authorized designees may use a CLETS Terminal.

303.4 RESPONSIBILITIES:

I. Department personnel authorized to use CLETS:

   A. Complete CLETS training as mandated by the DOJ. Maintain the integrity and security of CLETS through:

      1. Taking reasonable measures to locate equipment in a secure area.

      2. Only allowing authorized personnel to have access.

3. Obtain prior authorization from the Terminal Agency Coordinator and the CSA ISO, or their designee, before turning off/unplugging any CLETS terminals.

4. Obtain prior authorization from a Manager and/or Administration in coordination with the TAC and the CSA ISO /designee before relocating any CLETS terminal.

5. Maintain password integrity by:

   (a) Having a password from 8 to 20 characters.

   (b) Not using a dictionary word or proper name.

   (c) Not using the same password as the user ID.

   (d) Not being identical to the previous ten (10) passwords.

   (e) Changing password every 90 days.

   (f) Not allowing the password to be transmitted in the clear outside the secure location.

B. Report any indication of misuse, abuse or lost or stolen equipment, whether internal or external, to their immediate supervisor immediately. This includes, but is not limited to, unforeseen or unintentional access or use/abuse, cyber abuse, hacking, malware, etc.

C. Work in conjunction with the CSA ISO to determine the nature of the incident and determine whether CLETS access needs to be discontinued.

II. In the event of misuse, abuse, stolen equipment or suspected data compromise, whether internal or external, all Supervisors/Managers of the San Bernardino County Probation Department shall:

A. Report the incident immediately by phone or in person to:

1. The CJIS Systems Agency Information Security Officer (CSA ISO): The Department Information Services Administrator at office [redacted] or cell [redacted] OR

2. The Supervising Automated Systems Analyst II (SASAII) at office [redacted] cell [redacted], AND

3. The Terminal Agency Coordinator (TAC) at office [redacted].

B. Determine the location of any affected computers and immediately remove all network access from the affected machine(s), to include, but not limited to, removing network cables or air card. NOTE: IF POSSIBLE, AVOID TURNING THE CLETS TERMINAL OFF. Shutting the device down will cause any computer logs to be reset at the next logon and potentially lose critical information that may be used to mitigate the incident.

C. Direct the reporting party to prepare an inter-office memo immediately to include the following information:

1. The name and contact information of the reporting party.

2. The date and time the information was reported to their supervisor.
3. The date and time the incident was observed.
4. Equipment and all persons involved.
5. Location at the time of the incident.
6. A description of how the incident was detected.
7. Any supporting elements relating to the occurrence of the incident.

D. Deliver the inter-office memo to the TAC and CSA ISO as soon as completed.

III. In the event of misuse or abuse, whether internal or external, the CSA ISO and the TAC shall:

A. Determine the nature of the incident and determine whether CLETS access needs to be discontinued.

B. Contact Administration and Professional Standards and forward the abuse/ misuse report, if applicable.

IV. In the event of misuse or abuse, whether internal or external, the CJIS Systems Agency Information Security Officer (CSA ISO), or the SASAII shall:

A. Mitigate the issue, if possible, to avoid security breach or data loss.

B. At the conclusion of the incident or as available, provide administration with a report to include:

1. Cause of incident.
2. Type of incident.
3. How the issue was resolved.
4. Any mitigating issues.
5. Recommendations.

C. Preserve any evidence (event logs, emails, etc.).

D. Assess any damages or costs.

E. Review administration response and/or procedures for unnecessary updates or clarifications.

F. Implement recommendation upon written administration approval.

G. Complete the Security Incident Response Form (attachment A) under one of the following categories:

1. Category one - A threat to public safety or life.
2. Category two - A threat to sensitive data.
3. Category three - A threat to computer systems.
4. Category four - A disruption of services.

H. The CSA ISO /designee, and/or the TAC shall notify external agencies, if required:

1. DOJ.
2. CLETS Host Agency.
3. Affected persons, if personal information was compromised.

V. Automated Systems staff, at the direction of the CSA ISO or the SASAII, shall:

A. Determine the location of any affected computers and immediately remove all network access from the affected machine(s), to include, but not limited to, removing network cables or air card. NOTE: IF POSSIBLE, AVOID TURNING THE CLETS TERMINAL OFF. Shutting the device down will cause any computer logs to be reset at the next logon and potentially lose critical information that may be used to mitigate the incident.

B. Document:

1. The name of the Automated Systems Staff who was contacted.
2. Time of the contact.
3. Contact information for the Automated Systems Staff who was contacted.

C. Determine the following:

1. Type of Incident.
2. Equipment involved.
3. Location of the equipment.
4. Is the equipment business critical.
5. Name/IP Address of affect equipment.
6. Severity of incident.
7. Urgency of response.
8. Is the incident real or perceived.
9. Is the issue still on-going.
10. What data is at risk.
11. Was CLETS/CORI data compromised.
12. Business impact.
13. Is the incident coming from inside or outside the trusted network.

D. Take the following actions:

1. Mitigate the issue, if possible.
2. Review system logs on affected computers.
3. Consult with County Information Systems Staff on reviewing intrusion detection logs.

4. Provide the CSA ISO or the SASAII, with a report that includes, but is not limited to:
    (a) Cause of incident.
    (b) Type of incident.
    (c) How the issue was resolved.
    (d) Mitigating issues.
    (e) Recommendations.
5. Preserve any evidence (event logs, emails, etc.).
6. Assess any damages or costs.
7. Review response and procedures.
8. Implement recommendation upon written approval.

303.5 ATTACHMENTS:

See attachment: CLETS Incident Response Plan Attachment A (Lexipol 6-1-2019).pdf

Attachments

CLETS Incident Response Plan Attachment A (Lexipol 6-1-2019).pdf

F.1 Security Incident Response Form

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

_____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

_____

SYSTEM(S) AFFECTED: _____

_____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

_____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

_____

_____

Copies To:

[redacted]

(FBI CJIS Division ISO)

[redacted]

[redacted]