

Criminal Information Sharing Platform

438.1 PURPOSE AND SCOPE

The purpose of this Policy is to ensure that the San Leandro Police Department (“Department” or “Agency”) appropriately utilizes an internal information sharing platform to collect, evaluate, maintain and disseminate information regarding criminal activity that impacts the City of San Leandro (“City”). This system is not to be used as a multijurisdictional Criminal Intelligence System, nor should it contain Criminal Intelligence Files as the intended use of the platform is to share fact based information rather than intelligence products from data based on an analytic process as defined by 28 CFR Part 23. See definitions for clarification between Information and Intelligence as it relates to this Policy.

438.1.1 DEFINITIONS

Definitions related to this policy include:

Information - “Pieces of raw, unanalyzed data that identify persons, organizations, evidence, events or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.”

Intelligence - Raw information that is assessed for validity and reliability, reviewed for materiality to the issues at question, and given meaning through the application of inductive or deductive logic. Law enforcement intelligence, therefore, is “the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality.”

Criminal Information Sharing Platform (CISP) - Best practices dictate that a platform for sharing Criminal Information should take place on a secure CJIS (Criminal Justice Information Services) compliant system that receives, stores, exchanges, or disseminates information about criminal activity, officer safety or for another legitimate law enforcement purpose on a “need to know” and “right to know” basis. The Criminal Information Sharing Platform will be used as a secure platform that allows users to store, exchange and disseminate private or sensitive information about criminal activity, officer safety or for other legitimate law enforcement purposes.

Criminal Intelligence Information - Legally gathered factual data which has been analyzed to determine that it is relevant to the identification of, or the criminal activity engaged in by, person(s), groups, associations, or organizations.

Criminal Intelligence System - Any record system that receives, stores, exchanges or disseminates information that has been evaluated and determined to be relevant to the identification of a criminal organization or enterprise, its members or affiliates that meet the reasonable suspicion criteria and other operating principles as defined by 28 CFR Part 23.

Criminal Intelligence Files - Any files relating to a specific person, group, association, or organization which contains criminal intelligence information that demonstrates a criminal predicate exists as to the person, group, association, or organization. In this context “person” may include persons known to exist whose identities have not yet been ascertained.

San Leandro Police Department

San Leandro PD Policy Manual

Criminal Information Sharing Platform

Users are defined as employees of the Department who interact with, post on, utilize information on, or remove information from the CISP, including but not limited to Content Managers, Administrators, and Submitters as defined in this Policy.

438.2 POLICY

The San Leandro Police Department recognizes that information gathering is a fundamental and essential element in the duties of any law enforcement agency. When appropriately acquired, analyzed and shared, information is used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for conviction. It is the policy of this agency to gather and share information internally to enhance the Department's mission of protecting lives and property, collecting relevant evidence and further prosecution of subjects associated to criminal activity.

Information gathered will be directed toward specific individuals or organizations where there is reasonable suspicion that said individuals or organizations may be planning or engaging in criminal activity that affects the City of San Leandro. The information will be gathered with due respect for the rights of those involved and disseminated only to authorized individuals as defined under Section 424.11 Release of Information as specified in this Policy. It is also the policy of this Agency to adopt standards which are established to ensure the legality and integrity of the use of such an information sharing platform, which include:

- Procedures for ensuring information collected is limited to criminal conduct;
- Use of the platform as it relates to activities that pose a threat to the community;
- Descriptions of the types or quality of information that may be included in the system;
- Standards for purging out-of-date or incorrect information.

Information that is shared, or accessed, via the platform may include administrative messages related to police department business.

438.3 SECURITY

All Users must maintain the highest levels of security and confidentiality when using the platform. Users shall adhere to all applicable policies related to information technology use, electronic communications, records release, and protected information.

438.4 USE

All users of this agency are responsible for using the platform for sharing information in a timely manner for the purposes of:

- (a) Identifying and apprehending subjects associated to criminal activity;
- (b) Identifying threats to public and/or officer safety;
- (c) Supporting criminal investigations;
- (d) Furthering prosecution of subjects associated to criminal activity;

San Leandro Police Department

San Leandro PD Policy Manual

Criminal Information Sharing Platform

- (e) Addressing quality of life issues; to include but not limited to, encampments, blight and disorderly or disruptive public behavior;
- (f) Providing insights into emerging crime trends that impact the City.

Users shall maintain civil and privacy rights of all individuals at all times and only enter information that was obtained legally and appropriately.

All users must ensure that information entered is correct to the best of their knowledge and as timely as possible. Users should log onto the platform once per shift.

Along with this policy, each User shall be familiar with the City's guidelines for electronic communications in Administrative Procedure 1010.

438.5 PROCEDURE

Users must obtain the requisite training before accessing the platform. Training will include identification of information that may be particularly relevant for inclusion on the system. If entries are made based upon information that is not on file with this department, such as open or public source documents or documents that are on file at another agency, the submitter should ensure that sufficient information is included for reference or referral if needed in order to verify its accuracy. Examples include: Case number or contact information for outside agency cases or information, screenshots of open source or public source documents or contact information from the original source document/bulletin.

Once information is developed and identified as meeting the requirements for entry, Department members should enter information into the platform appropriately and in a timely manner.

Examples of relevant information includes, but is not limited to:

- (a) Information related to subjects involved in criminal activity;
- (b) Gang indicia or vandalism associated with a person or residence;
- (c) Information related to problem locations such as bingo halls or illegal gambling operations;
- (d) Information relating to crime trends;
- (e) Officer safety information;
- (f) Beat health information.

Information entered should be checked for validity, authenticity, accuracy and reliability. Corroborative evidence should be sought and documented in the related investigative report if appropriate. It is the responsibility of the person submitting the information to ensure that they clarify if there is any action that needs to be taken based upon the information submitted. This may include:

- (a) Arrest of a wanted subject;
- (b) Extra patrol checks for suspicious activity;
- (c) No contact desired due to UC (undercover) operations;

San Leandro Police Department

San Leandro PD Policy Manual

Criminal Information Sharing Platform

- (d) Probation or parole search.

Information and documents added to the platform:

- (a) Shall not be originals that would ordinarily be retained by the Records Unit or Property and Evidence Section, but should be copies of, or references to, retained documents such as copies of reports, FI forms, the Communications Center records or booking forms.
- (b) Shall not include opinions. No person, organization or enterprise shall be labeled as being involved in crime beyond what is already in the document or information.
- (c) Shall not include screenshots of California Law Enforcement Telecommunications System (CLETS) returns, Consolidated Records Information Management System (CRIMS) dockets, Department of Motor Vehicles (DMV) records, California Information & Identification (CII) number, etc. with identifying information in order to maintain Criminal Offender Record Information (CORI) protections. Please summarize in body of post. Photographs (i.e., mugshots) alone are acceptable.
- (d) Shall not include informant information.
- (e) Shall be confirmed prior to arrest or apprehension in the case of warrants, probation and/or parole.
- (f) If stating subject is on probation, please refer to docket and expiration date. If you see a post without this information, please confirm docket and expiration date before taking action.

If there is a violent felony with a callout initiated, the person's crimes sergeant shall be contacted and approval sought prior to adding information regarding the callout in the platform. Specific folders may be created that limit access to platform based upon job assignment and duties.

438.6 PROHIBITED USE

Users will consider protection of individual civil rights at all times. Only information with a criminal nexus, public/ officer safety concern or significant quality of life issue which meets the criteria for input should be included. Information pertaining solely to religion, gender, race, sexuality, politics or any other protected class without a criminal, or public safety, nexus is prohibited. Any information that is deemed inappropriate or falls under prohibited use shall be immediately removed and reported to the appropriate supervisor.

Specifically excluded material includes:

- (a) Information on an individual or group merely on the basis that such individual or group supports unpopular causes.
- (b) Information on an individual or group merely on the basis of ethnic background.
- (c) Information on any individual or group merely on the basis of religious or political affiliations.
- (d) Information on an individual or group merely on the basis of sexual identity or orientation.

San Leandro Police Department

San Leandro PD Policy Manual

Criminal Information Sharing Platform

- (e) Information on an individual or group merely on the basis of non-criminal personal habits.
- (f) Information copied directly from the Criminal Offender Record Information (CORI), shall be excluded from the platform. This is because CORI may be subject to specific audit and dissemination restrictions which are designed to protect an individual's right to privacy and to ensure accuracy. CORI information may be summarized within the platform.
- (g) Also excluded are associations with individuals that are not of a criminal nature.

Any User who becomes aware of content on the platform that he/she believes is unauthorized or inappropriate shall promptly report such content to their immediate supervisor, or a CISP supervisor or administrator. The supervisor will ensure its removal from platform and investigate the cause of the entry.

User shall not refer to obtaining information contained in the platform in police reports.

438.7 DATA RETENTION

The retention period for all information input into CISP shall not exceed five years. Information will be automatically purged from the platform by the expiration of its retention period, unless the information has been interacted with by a platform user.

The Criminal Information Sharing Platform Administrator is responsible for ensuring that the platform is maintained in accordance with the goals and objectives of the Department and includes information that is both timely and relevant. To that end, the system shall be monitored for inappropriate content and if information is posted that violates policy it will be removed as quickly as possible.

All information entered into the platform is for official use only, and because such data may contain confidential information, it is not open to public review. Information gathered and retained by in the platform may be used and shared with prosecutors or others only as permitted by law, or on a "need to know," "right to know" basis.

438.8 ROLES AND RESPONSIBILITIES

The roles and responsibilities for use of the Criminal Information Sharing Platform are as follows:

438.8.1 CRIMINAL INFORMATION SHARING PLATFORM ADMINISTRATOR

The Chief of Police will appoint a Sharing Platform Administrator to review, at least annually, the Department's use of the internal criminal information sharing platform and report back on, at a minimum, the resources being used, and the effectiveness of the content, any unauthorized or inappropriate content, and the resolution of any issues. The CISP Administrator will also ensure that data retention and purge schedules are maintained.

In addition, the Administrator shall ensure the following:

- (a) Users of the platform are appropriately trained and have access to appropriate folders within system;

San Leandro Police Department

San Leandro PD Policy Manual

Criminal Information Sharing Platform

- (b) Platform content is appropriately reviewed and audited;
- (c) Any system security issues are reasonably addressed;
- (d) Best practices for information sharing, platform use, and civil and privacy rights are maintained;
- (e) Updating passwords or login information as needed;
- (f) Providing training and resources to users as needed.

438.8.2 CRIMINAL INFORMATION SHARING PLATFORM SUPERVISOR

The Chief of Police will appoint a CISP Supervisor to assist the CISP Administrator with reviewing the Department's use of the internal criminal information sharing platform and report back on, at a minimum, the resources being used, and the effectiveness of the content, any unauthorized or inappropriate content, and the resolution of any issues.

In addition, the Supervisor will be assigned with:

- (a) Reviewing platform for unauthorized or inappropriate content;
- (b) Acting as a backup to the CISP Administrator as needed.

438.8.3 CONTENT MANAGERS

Content Managers are members assigned to the Criminal Investigative Division (CID) or are involved in the role of an Intelligence Officer and are responsible for assisting with the management of content as it relates to their role. They will assist with:

- (a) Ensuring that information related to their cases or information obtained from their role as an Intel Officer is added to the appropriate folder and/or thread;
- (b) Providing information and updates on outstanding subjects, vehicles or significant case data in a timely manner;
- (c) Providing clear instructions for any action needed on information provided.

438.8.4 SUBMITTERS

Submitters are all other members who are not assigned another role. They are responsible for:

- (a) Logging into the platform once per shift;
- (b) Creating and posting any notable criminal incident for department awareness as soon as they are able during their shift;
- (c) Providing updates to any actions on information taken during shift.

Submitters may not purge information from platform without the approval of the designated CISP Supervisor or Administrator.

438.9 RELEASE OF INFORMATION

Department members shall comply with the rules regarding authorized release of information and may only share information with other law enforcement agencies on a "need-to-know" and "right-to-know" basis which is consistent with the Protected Information Policy (Lexipol Policy 806). Users

San Leandro Police Department

San Leandro PD Policy Manual

Criminal Information Sharing Platform

may only share and provide information that is accurate and appropriate. All efforts must be made to adhere to the confidentiality of the information contained in the platform. In order to maintain the integrity of the system screenshots are not allowed and printing from the platform is prohibited and will be disabled.

438.10 TRAINING

Users shall receive training that, at a minimum, addresses legal issues concerning the appropriate use of the platform, as well as privacy, civil rights, dissemination and retention of information posted to the platform.

The Professional Standards and Training Unit, with the assistance of the supervisor, shall provide training on best practices in the use of the platform. Training should include:

- (a) The protection of civil liberties;
- (b) Submission of information into the platform;
- (c) The type of information appropriate for entry into the platform;
- (d) The review and purging of information and retention policies.

438.11 RESCINDED POLICY

This Policy rescinds San Leandro Operations Directive 92-01.

I understand that it is my responsibility to review, become familiar with and comply with all the provisions of this new or updated Policy. I further understand that, if I have questions about or do not fully understand any portion of this Policy, it is my responsibility to seek clarification from my supervisor. I hereby acknowledge that I have received, read and understand this Policy.

Intelligence and Information definitions come from "Law Enforcement Intelligence: A guide for State, Local, and Tribal Law Enforcement Agencies"- US Department of Justice Table 2-1 p.12.