DEPARTMENTAL GENERAL ORDER

I-24: FORENSIC LOGIC COPLINK

Effective Date:

Coordinator: Information Technology Unit

FORENSIC LOGIC COPLINK

The purpose of this order is to establish Departmental policy and procedures for the use of the Forensic Logic, LLC. CopLink Data System

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of the Forensic Logic, LLC. CopLink law enforcement data search system. The Oakland Police Department (OPD) uses crime databases to provide OPD personnel with timely and useful information to investigate crimes and analyze crime patterns.

A. Purpose: *The specific purpose(s) that the surveillance technology is intended to advance*

Forensic Logic, Inc. ("Forensic Logic") built a data warehouse that integrates and organizes data from databases such as Computer Assisted Dispatch (CAD) and Records Management System (RMS) and other law enforcement information systems from different law enforcement agencies. Forensic Logic provides two core services for OPD: 1) crime analysis reports; and 2) data search.

1. Crime Analysis Report Production – Forensic Logic categorizes and organizes incidents by offense types that allows OPD crime analysts to produce crime analysis reports such as point in time year-to-date and year-to-year comparisons. The categorization takes thousands of penal code types and organizes the data in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Report Part One and Part Two crimes.
2. Search – OPD data (e.g., CAD/RMS) is searchable with other agency law enforcement data. Personnel can use the system to search crime reports for structured data (e.g., suspect names) and unstructured data (e.g., a vehicle description). The cloud-based search system is accessible via a secure internet web browser requiring user authentication from vehicle mobile data terminal (MDT), web-enabled computers on the OPD computer network, or via OPD-issued and managed mobile devices.

B. Authorized Use*: The specific uses that are authorized, and the rules and processes required prior to such use*

The authorized uses of Forensic Logic system access are as follows:

- Crime Analysis Report Production – Authorized members may use the customized system to organize OPD crime data into Crime Analysis Reports. Forensic Logic built a system that categorizes thousands of penal codes based on hierarchical crime reporting standards, into a concise, consumable report template.
- CopLink Search – Authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Rules and Processes Prior to use

- Only sworn law enforcement personnel or authorized professional staff employed and working under the supervision of a law enforcement agency (typically crime analysts and dispatchers) may access the Forensic Logic CopLink network.
- OPD personnel authorized to use Forensic Logic CopLink receive required security awareness training prior to using the system. Forensic Logic requires users to have the same training to access the Forensic Logic CopLink network as users are required to be trained to access data in CLETS, the FBI NCIC system or NLETS. Users are selected and authorized by OPD and OPD warrants that all users understand and have been trained in the protection of Criminal Justice Information (CJI) data in compliance with FBI Security Policy. All Forensic Logic CopLink users throughout the Forensic Logic CopLink network have received required training and their respective law enforcement agencies have warranted that their users comply with FBI CJI data access requirements.
- Users shall not use or allow others to use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to investigations, internal audits, or for crime analysts to produce crime analysis reports. The purpose of the Forensic Logic CopLink network is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. Users are required to abide by the Terms of Service of the Forensic Logic CopLink network when they access the system. The Terms of Service that every User agrees to include the following statements:
    1. *I will use the Forensic Logic Coplink Network™ only for the administration of criminal justice or the administration of data required to be stored in a secure sensitive but unclassified data environment.*

2. *I will respect the confidentiality and privacy of individuals whose records I may access.*
3. *I will observe any ethical restrictions that apply to data to which I have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information.*
4. *I agree not to use the resources of the Forensic Logic Coplink Network™ in such a way that the work of other users, the integrity of the system, or any stored data may be jeopardized.*

I am forbidden to access or use any Forensic Logic Coplink Network™ data for my own personal gain, profit, or the personal gain or profit of others, or to satisfy my personal curiosity.

- The following warning is displayed for every user session prior to user sign on:

  WARNING: *You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report or other information exists in the Records Management System or other law enforcement, judicial or other information system of an identified participating agency or business.*

  In accordance with California Senate Bill 54, applicable federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

- Accessing CopLink data requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in a criminal investigation.

C. ***Data Collection:*** *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;*

Forensic Logic has created a file transfer protocol to automatically ingest several data systems into the Forensic Logic CopLink system. These databases include

CAD/RMS and FBR. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system. No ALPR data collected by OPD-owned technology shall be extracted by Forensic Logic's systems. An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	**Collection Status**	**Retention Policy**	**Access Conditions**
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited
Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

There are several "Elements of the Search" component – all of which are specialized presentations of search[1]: (see related Surveillance Impact Report for a detailed analysis:

- The search bar;
- The Tag Cloud element - how search results are visualized by increasing the font size in a Tag Cloud to be representative of the number of occurrences;
- Facet search - organizes search capabilities into a number of static

[1] See related Surveillance Impact Report for a detailed description of each 'search' module

categories (e.g. offense descriptions, agencies);

- Time Search - permits users to quickly drill down to specific time periods;
- Timeline search - organizes the data visually on a timeline;
- Geospatial search - permits a user to select geographies (e.g. Beats or Areas; areas around schools, custom areas);
- Search Charting Module - organizes search results into categories visualized by bar charts;
- Link Chart - produces a visualization of records that are linked based on several criteria including name, offense and location.

Forensic Logic CopLink also consists of the following modules:

- CopLink Connect (formerly called forums);
- CopLink Dashboard, and CopLink Trace (gun-tracing);
- CopLink Connect - a secure internal communication system for intra-agency CJIS-compliant communications.

D. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information*

Authorized users include all sworn personnel, Crime Analysts, Police Evidence Technicians, personnel assigned to OIG, and other personnel as approved by the Chief of Police.

OPD data in the Forensic Logic CopLink system is owned by OPD and not Forensic Logic and is drawn from OPD underlying systems. OPD personnel shall follow all access policies that govern the use of those originating OPD technologies.

OPD's Information Technology (IT) Unit shall be responsible ensuring ongoing compatibility of the Forensic Logic CopLink System with OPD computers and MDT computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and coordinate with Forensic Logic. CopLink Search users are managed through a centralized account management process by Forensic Logic support personnel.

E. Data Protection: *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;*

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI

Security Management Act of 2003 and CJIS Security Policy. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

F. Data Retention*: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

Forensic Logic follows the data retention schedules reflective of OPD's data retention schedules. Data that is deleted from OPD CAD/RMS or other systems will be automatically deleted from Forensic Logic CopLink system. OPD can also request that OPD data be expunged from the Forensic Logic CopLink system where appropriate based on changes to incident files.

G. Public Access*: How collected information can be accessed or used by members of the public, including criminal defendants;*

The Weekly Crime Analysis Reports prepared using Forensic Logic's analysis of OPD crime data are regularly made available to the public on OPD's website. The CopLink system is only provided for OPD personnel and is not available to the public.

H. Third Party Data Sharing: *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;*

Other than selected individuals with a right to access at ITD, no other non-OPD City entities may access the Forensic Logic system. Many law enforcement agencies (city police departments and county sheriff offices) utilize Forensic Logic CopLink. ***Attachment A*** to this Use Policy provides a list of agencies[2] that are clients of Forensic Logic and have access to OPD data through CopLink Search.

Many law enforcement agencies that are clients of Forensic Logic have access to OPD data through CopLink – a complete list is provided in ***Appendix D*** to the CopLink Surveillance Impact Report.

[2] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

I. Training: *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;*

OPD's IT Unit shall ensure the development of training regarding authorized system use and access.

J. Auditing and Oversight: *The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and*

The OPD IT Unit will manage audit requests in conjunction with Forensic Logic, Inc.

Per FBI CJIS Security Policy, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;
    b. modify the audit log file;
    c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.

3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

OPD's IT Unit shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of Forensic Logic's CopLink and Crime Reporting modules during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

K. Maintenance: *The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.*

Forensic Logic, Inc. shall be responsible for all system maintenance per the OPD-Forensic Logic, Inc "software as a service" or (SAAS) contract model.

By Order of

Susan E. Manheimer

Chief of Police Date Signed: