LACRIS

LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

Facial Recognition Policy

V 1.2

Revised 01.01.23

Contents

A. Preface

The Los Angeles County Regional Identification System (LACRIS) has developed a policy that should be the foundation for member agencies that utilize the LACRIS facial recognition (FR) system. LACRIS is responsible for the governance, oversight, and operation of its FR system and program, which it provides to the law enforcement community within Los Angeles County. This policy is intended for LACRIS personnel and any authorized agency personnel accessing the system. Effective July 1, 2023, agencies must implement their own policy, which complements but does not contradict this LACRIS FR policy. Agencies that fail to enact policies will have their access to the Facial Recognition application suspended until a policy is in place. An FR policy template can be obtained through the LACRIS Help Desk at lacrishd@lasd.org or the LACRIS website at www.lacris.org.

B. Purpose Statement

FR technology can be a valuable tool to create investigative leads, reduce an imminent threat to health or safety, and help in the identification of deceased persons or persons unable to identify themselves. The LACRIS FR application supports the investigative efforts of law enforcement and public safety agencies within Los Angeles County and resides in the County's Digital Mugshot System (DMS).

C. Digital Mugshot System

Established October 1, 2009, the DMS is the County's repository of all criminal booking photos (mugshots). It only contains criminal booking photos, which are supported by a fingerprint comparison conducted by the California Department of Justice (DOJ). Section 13150 of the California Penal Code requires a subject's fingerprints and associated arrest data to be collected, stored, and reported to the DOJ at the time of booking. This information is maintained in the DMS and used by authorized law enforcement personnel for investigative purposes.

D. Authority

All deployments of the DMS FR application are for official use only and are considered law enforcement sensitive. The DMS is subject to the DOJ regulations placed on users and the dissemination of Criminal Offender Record Information (CORI).

The California Attorney General's Office issued Information Bulletin 13-04-CJIS, which guides law enforcement personnel on "right to know" and "need to know" access to CORI for investigative and official business purposes. This Bulletin references the relevant statutory codes (see below) that must be adhered to by users accessing the system.

Section 11075 of the California Penal Code (PC) defines CORI as "records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release."

Section 11105 of the PC identifies who has access to DOJ CORI and under what circumstances it may be released. Access is based upon the "right to know" and the "need to know." The "right to know" is defined as "authorized access to such records by statute," and the "need to know" is defined as "the information is required for the performance of official duties or functions." Title 11, sections 703 (d) and 707 (b) of the California Code of Regulations (CCR) require agencies to conduct record clearances on all personnel hired who have access to CORI. The unauthorized access and misuse of CORI violates state statutes and may adversely affect an individual's civil rights. Sections 11140 through 11144 of the PC prescribe penalties for misuse of state summary criminal history information, while PC sections 13301 through 13304 prescribe penalties for misuse of local summary criminal history information. Sections 6200 and 6201 of the Government Code prescribe the penalties for the misuse of various government records, which include CORI. Section 502 of the PC defines the penalties relating to computer crimes.

Title 11, section 707 (c) of the CCR requires each authorized agency to maintain, and make available for inspection, an audit trail for a period of three years from the date of release of CORI from an automated system. The audit trail must provide an agency with sufficient information to substantiate the "need to know."

Section 11078 of the PC requires each agency holding or receiving CORI in a computerized system to maintain a listing (audit trail) of the agencies to which it has released or communicated CORI. Also, pursuant to section 707 (c) of the CCR, this audit trail must be maintained for a period of three years and must include any routine releases.

All code sections, which may be amended from time to time, are current as of the time of the implementation of this policy.

E. Prohibited Uses

The DMS allows access to booking repositories only and is not capable of connecting to any live video stream or surveillance system.

In accordance with Cal-DMV Practices, Policies, and Procedures, California DMV images shall not be saved or downloaded to create a local database or used for facial recognition purposes (Cal-Photo version: CP 7.21).

F. Training

LACRIS provides training to users whose agency authorizes access to the FR application for official use. Personnel must be successfully trained by LACRIS personnel or have previously attended FR training which meets the FBI's minimum training criteria for using FR systems. The FR training provided by LACRIS meets the FBI's Criminal Justice Information Services (CJIS) minimum criteria for using FR systems. Personnel who provide proof of FBI equivalent training not provided by LACRIS must have attended the training after January 1, 2017.

G. Auditing

LACRIS will ensure that the DMS technology complies with the current CJIS Security Policy regarding audits. The DMS automatically audits user actions such as login time, date search, subject viewed, etc. LACRIS personnel will conduct random audits of users and report their findings directly to the agency when their users are not in compliance. LACRIS audits users' search and activity compliance, including search reason, number of searches, subject status, watch list entries, etc. (See below for compliant and non-compliant search reason examples). Audit report data will be compiled and stored at LACRIS for three (3) years. All audits and subsequent reports are subject to disclosure under the California Public Records Act. Agencies are required to conduct quarterly audits of their trained personnel's usage and notify LACRIS of any changes to their access privileges.

Compliant Search Reasons

- John Smith housing, BK#1234567
- Case# 123-89765-0123-41X, 211 PC
- Wristband Verification, BK#7654321
- Release Citation, #ABC-123
- Incident / Tag #567

Non-Compliant Search Reasons

- Investigation
- Positive ID
- Housing
- 211 PC
- Verify

H. Accountability and Enforcement

LACRIS maintains several applications that must adhere to regulations and laws, including user access. Corrective action must be taken if LACRIS determines a violation of these regulations or laws has occurred. Depending on the severity of the violation, LACRIS will hold users accountable for their actions. Penalties include but are not limited to restricted access, revoked access, and prosecution. Users may also be subject to additional discipline from their respective agency and other law enforcement agencies, including but not limited to State or Federal agencies.

I. Face Search Requests

Agencies without an FR system may request a face search to assist with an investigation by submitting the "LACRIS Facial Recognition Search Request form." This form can be obtained through the LACRIS Help Desk at lacrishd@lasd.org and will require the following information:

- Requesting Agency
- Requester Name
- Requester Phone Number
- Requester Email
- Requester Signature
- Date of request
- Reason for Search
- Case/File Number
- Where the source image was obtained
- Was the source image extracted from a video
- Number of Images Submitted

LACRIS personnel will review each request before processing the search to ensure compliance with this policy. Requesters acknowledge that the result of any FR search provided by LACRIS shall be deemed an investigative lead only. RESULTS ARE NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.