LACRIS

LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

Facial Recognition Policy

V 1.1

Revised 09.01.21

Contents

A. Preface

The Los Angeles County Regional Identification System (LACRIS) has developed a policy that shall be used as the foundation for those agencies that choose to 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 the county of Los Angeles. This policy is intended for LACRIS personnel and any authorized agency personnel accessing the system. Agencies are encouraged to implement their own policy which complements and does not contradict this LACRIS policy.

B. Purpose Statement

FR technology involves the ability to examine and compare significant characteristics of the human face. This 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. This FR application supports the investigative efforts of law enforcement and public safety agencies within Los Angeles County 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 at time of booking, a subject's fingerprints and associated arrest data to be collected, stored, and reported to the DOJ. This information is maintained in the DMS and used for investigative purposes by authorized law enforcement personnel.

D. Authority

All deployments of the DMS FR application are for official use only and 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 provides guidance to law enforcement personnel on “right to know” and “need to know” access to CORI for investigative and official business purposes. This Bulletin, while not legally binding, 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 ACHS and 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 prescribes 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 stream video or surveillance system. Additionally, use of video and/or still images obtained from body worn cameras or similar devices are prohibited under section 832.19 of the California state Penal Code.

F. Training

LACRIS provides training to users who are authorized by their agency to access 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 usage of FR systems. The FR training provided by LACRIS meets the FBI's Criminal Justice Information Services (CJIS) minimum criteria for usage of 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 provided complies with the then current CJIS Security Policy in regard to audits. The DMS automatically audits user actions such as, logon time, date search, subject viewed, etc. LACRIS personnel will conduct random audits of users and report their findings directly to the user's agency. LACRIS audits user's search and activity compliance to include search reason, number of searches, subject status, watch list entries, etc. Audit report data will be complied and stored at LACRIS for a minimum of three (3) years. Agencies are required to conduct monthly audits of their trained personnel's usage and forward those reports quarterly to LACRIS.

H. Accountability and Enforcement

LACRIS maintains several applications that must adhere to regulations and laws which includes user access. Through audits, if LACRIS determines there was misuse or a violation of these regulations and/or laws, it must take corrective action. Depending on the severity of the violation, LACRIS will hold those user(s) accountable for their actions. Penalties may include but are not limited to restricted access, revoked access, or prosecution. Users may also be subject to additional discipline from their respective agency, as well as other law enforcement agencies, including but not limited to State or Federal agencies.

I. Face Search Request

Investigators from outside agencies, may request FR searches to assist with investigations through LACRIS only if the LACRIS *Face Recognition Search Request Form* is completed. This form can be obtained through the LACRIS Help Desk at lacrishd@lasd.org and will require the following minimum information:

- Requesting Agency
- Requester Name Requester Phone Number
- Requester Email
- Requester Signature
- Requester Date
- Reason for Search
- Case/File Number
- Number of Images Submitted

LACRIS personnel will review each request prior to processing to ensure compliance with this policy. Users acknowledge the result of any FR search provided by LACRIS shall be deemed an investigative lead only and RESULTS ARE NOT TO BE CONSIDERED AS PROVIDING 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.