LACRIS

LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

Facial Recognition Policy

V 2.0 06/23

Table of Contents

Preface 3
Purpose Statement 3
Digital Mugshot System (DMS) 3
Authority 3
Definitions 4
Prohibited Uses 4
Training 4
Audits 5
Data Retention 5
Accountability and Enforcement 5
Face Search Requests 6

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 for LACRIS personnel and any authorized agency or agency personnel accessing the system. Effective July 1, 2023, agencies must implement their policy, which complements but does not contradict this LACRIS FR policy. Agencies that fail to enact policies will have access to the Facial Recognition application suspended until a policy is in place. For assistance, member agencies can obtain an FR policy template through the LACRIS Help Desk at lacrishd@lasd.org or the LACRIS website at www.lacris.org.

Purpose Statement

FR technology can be a valuable tool to create investigative leads, reduce an imminent threat to health or safety, and help identify deceased persons or persons unable to identify themselves. The LACRIS FR system 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).

Digital Mugshot System (DMS)

Established October 1, 2009, the DMS is the County's repository of all criminal booking photos (mugshots). It contains only criminal booking photos, supported by a fingerprint comparison conducted by the California Department of Justice (DOJ) and locally within LA County. California Penal Code § 13150 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.

Authority

This policy is established under the mandate of the Regulations Regarding Security of Criminal Offender Record Information in California, Title 11, California Code of Regulations. Other authorities include Penal Code § 11105, which defines who has access to Criminal Offender Record Information (CORI), and Penal Code § 11140 through § 11144, which establishes penalties for the improper use of CORI. All of which are incorporated hereby reference.

All deployments of the DMS FR system are for official use only and are considered law enforcement sensitive. Therefore, users must abide by both the DOJ CORI laws (DOJ Information Bulletin 19-04-CJIS) as well as the FBI's Criminal Justice Information Services (CJIS) Security Policy Version 5.9.1 (10/01/2022) as outlined in the LACRIS Terms of Use. The LACRIS Terms of Use are available on the LACRIS website at www.lacris.org and are incorporated herein by reference.

Definitions

Authorized Recipient - Any person or agency authorized by court order, statute, or case law to receive CORI and whose access is based upon the "need to know" and the "right to know".

Criminal Offender Record Information - records and data compiled by criminal justice agencies for purposes of identifying criminal offenders. For each offender, CORI may include a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, and information pertaining to sentencing, incarceration, rehabilitation, and release. Criminal justice agencies throughout the state provide this information to the DOJ, which is required to maintain it in a statewide repository. CORI includes manual/automated Records of Arrests and Prosecutions (RAP) sheets and abstracts, crime summaries, criminal history transcripts, FBI RAP sheets, and local law enforcement databases that are not accessible to the public.

Criminal Justice Agency - A public agency or component that performs a criminal justice activity as its principal function.

Facial Recognition – The automated searching of a facial image (probe) against a known collection database(s), resulting in a list of candidates ranked by computer-evaluated similarity score. This is commonly referred to as a one-to-many data-model comparison.

Facial Reviewer – A person who completed the FBI or LACRIS training in facial comparison.

Probe – The facial image or template that is searched against a known mugshot database in a facial recognition system.

Prohibited Uses

CORI shall not be accessed violating any law, order, regulation, user agreement, policy, or training. Personnel must be successfully trained by LACRIS or have previously attended FR training which meets the FBI's minimum training criteria for using FR systems. Only those users who have completed approved training and met any other applicable requirements, such as a background check, may access CORI, and only when the user has a right-to-know and need-to-know for such access.

The DMS allows access to booking repositories only and cannot connect to any live video stream or surveillance system.

Per Cal-Photo Policies, Practices, 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).

Training

LACRIS provides training to users whose agency authorizes access to the FR system for official use. 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 offered by LACRIS must have attended the training after January 1, 2017, to maintain access to the FR system.

Audits

The DMS complies with the current CJIS Security Policy regarding audits. The DMS keeps a detailed audit log (user action data) that automatically logs user actions such as login time, date of search, subjects viewed, etc. Each agency is responsible for identifying a local administrator to assist in auditing their users' actions within the DMS. The local administrator must conduct monthly audits of all DMS user actions to ensure lawful access and prevent misuse. In addition, local administrators are required to conduct quarterly audits of their personnel access privileges and ensure inactive user accounts are disabled.

Users must include a valid search reason within the DMS when conducting a search (See below for compliant and non-compliant search reason examples).

Compliant Search Reason

- 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 Reason

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

Monthly audits must be retained for five (5) years by a local administrator and submitted to LACRIS upon request. Audit templates can be obtained from LACRIS for use by the local administrator.

All local administrator-conducted audit reports will be audited monthly by LACRIS personnel.

Data Retention

Local administrator audit reports and user action data will be retained for five (5) years. All audits and subsequent reports are subject to disclosure under the California Public Records Act.

Accountability and Enforcement

Audits must be conducted by both local administrators and LACRIS to ensure compliance with laws, regulations, and policies described under this policy. Corrective action must be taken if LACRIS or the local administrator determines a violation of these laws, regulations, or policies has occurred. Penalties include but are not limited to re-training, restricted access, revoked access, or prosecution.

Users may be subject to additional discipline from their respective agencies and other law enforcement agencies, including but not limited to State or Federal agencies.

Face Search Requests

Agencies without an FR system may request a face search to assist with an investigation by submitting a completed "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.