

Facial Recognition System

600.1 PURPOSE AND SCOPE

This policy establishes procedures for the acceptable use of the Integrated Law and Justice Agency of Orange County (ILJAOC) Facial Recognition System (FRS), its images, information, and tools. The FRS shall only be used when there is reasonable suspicion that such use will provide information relevant to an active investigation, reduce an imminent threat to health or safety ("at-risk"), or to help identify deceased persons or persons unable to identify themselves. The FRS will be used in accordance with federal and state law, including the California Values Act (Government Code Section 7282 et. seq.).

The provisions of this policy are provided to support the authorized uses of the FRS and information identified below. This policy applies to all law enforcement agencies and agency personnel with access to the FRS, and access to the Investigative Leads produced therefrom. Each law enforcement agency requesting access to the FRS is required to maintain an internal policy regarding the use of the technology that is consistent with this policy and is expected to include agency specific operational procedures, as appropriate. Agencies that do not adopt internal policies and procedures consistent with this policy will not be granted access to the FRS. Any ambiguity or inconsistencies in the required policies shall be resolved in favor of a meaning that complies and is consistent with federal and state laws, regulations, and standards.

The ILJAOC considers the results, if any, of a Facial Recognition search to be an Investigative Lead only. Facial Recognition search results are not regarded as positive identification of a subject and do not, on their own, establish either reasonable suspicion to detain or probable cause to support a search warrant or an arrest. Connection or involvement of the subject(s) to the investigation must be determined through further lawful investigative methods and investigative resources (e.g., witness interviews, forensic analysis of crime scene evidence, witness or victim identification, etc.).

600.1.1 DEFINITIONS AND TERMS

Breach – The unauthorized acquisition, access, use, or disclosure of Facial Recognition data in a manner that compromises the security, confidentiality or integrity of the information; or the same as the definition of "breach of the security of the system" set forth in California Civil Code Section 1798.29(f).

Candidate Images – The results of a Facial Recognition search. When Facial Recognition software compares a Probe Image against the images in a Repository, the result is a list of Candidate Images that the software determines to be sufficiently similar to or most likely resemble the Probe Image to warrant further analysis. A Candidate Image is an Investigative Lead only

Facial Recognition System

and does not establish reasonable suspicion or probable cause without further investigation or evidence.

Facial Recognition – The automated process whereby a Probe Image is used by Facial Recognition software for comparison with the Known Images (or features within images) contained in the image Repository, resulting in a list of Candidate Images ranked by computer-evaluated similarity score. This is commonly referred to as a one-to-many comparison.

Facial Reviewer – The human reviewer of Candidate Images produced by the automated FRS to identify possible matches. The Facial Reviewer must have successfully completed training in facial comparison and use of the Facial Recognition software.

Investigative Lead – Any information that could potentially aid in the successful resolution of an investigation. An Investigative Lead does not imply positive identification of a subject, nor that the subject is responsible for or otherwise involved in a criminal act.

Known Image – The image of an individual associated with a known or claimed identity and recorded electronically by a law enforcement agency through the Orange County Automated Biometric Identification System during the individual's booking process at an Orange County or City Jail.

Log(s) – A necessary part of an adequate security system which ensures that information is properly tracked and that only authorized individuals have access to the data within the FRS and the resulting Candidate Images.

Participating Agency – A law enforcement agency that is authorized to contribute images and/or biometric information and/or is authorized to access, receive, request, or use information from ILJAOC's FRS for a Valid Law Enforcement Purpose through its authorized individual users. Participating Agencies must sign the Participating Agency Agreement (Agreement) with ILJAOC regarding the use of the FRS and adopt internal policies and procedures for use of the FRS that are consistent with this policy.

Personally Identifiable Information (PII) – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual.

Probe Image – The facial or distinctive image of a scar, mark or tattoo, used by Facial Recognition software for comparison against a Known Image contained within the FRS. The Probe Image must be an image of an individual lawfully obtained pursuant to a criminal investigation. Examples of Probe Images include:

- Images captured from closed circuit TV cameras or security cameras
- Images captured from an ATM camera.
- Images provided by a victim or witness of a crime.
- Images gained from a criminal investigation determined to be evidence of identity (fraudulent bank card or photograph ID).

Facial Recognition System

Repository – A location where a group of images of known individuals and biometric templates obtained and verified from the Orange County Automated Biometric Identification System through a law enforcement process are stored and managed. A Repository is utilized during a Facial Recognition search. A Repository may be referred to as a Digital Mugshot System (DMS) by other law enforcement agencies or groups.

Security Incident – An attempted breach; the attempted or successful unauthorized access or disclosure, modification, or destruction of Facial Recognition data in violation of any law or in a manner not permitted under this policy or the Agreement; or the attempted or successful modification or destruction of, or interference with, law enforcement operations in an information technology system that negatively impacts the confidentiality, availability, or integrity of Facial Recognition data.

Surveillance – Observation and collection of data to gather evidence.

Unsolved Image File – A lawfully obtained Probe Image of an unknown subject may be added by authorized law enforcement users to an unsolved image file pursuant to an authorized criminal investigation and if a search has produced no candidates and the subject remains unknown. Images in an unsolved image file are periodically compared with the Known Images in an image Repository.

Valid Law Enforcement Purpose – Facial Recognition is to be used for information/intelligence gathering, development, collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency. These functions and activities may include preventing crime, criminal investigation, criminal intelligence, mitigating imminent threats, ensuring public safety, protecting public or private structures and property, identifying deceased persons or persons unable to identify themselves, and furthering officer safety while adhering to law and agency policy designed to protect the public.

600.2 POLICY

The policy of the ILJAO is to utilize Facial Recognition technology as an investigative tool during investigations, reducing imminent threats to health or safety, or helping identify deceased persons or persons unable to identify themselves, while recognizing the established privacy rights of the public.

Facial Recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. California Penal Code § 13150 requires a subject's fingerprints and associated arrest data to be collected, stored, and reported to the California Department of Justice (DOJ) at the time of booking. This information is maintained in the Repository and used by authorized law enforcement personnel for Valid Law Enforcement Purposes. Facial Recognition technology can be a valuable investigative tool to detect criminal activity, reduce an imminent threat to health or safety, and identify deceased persons or persons unable to identify themselves. The ILJAO has established access to and use of a Facial Recognition software to support investigative efforts to solve crimes. The software will be treated like any other Investigative Lead and shall not be

Facial Recognition System

used as a sole guarantee of identification, reasonable suspicion to detain, or probable cause to search or arrest.

This policy provides the ILJAOC and law enforcement personnel with guidelines and principles for collecting, accessing, using, disseminating, retaining, and purging images and related information applicable to FRS. This policy will ensure that all Facial Recognition searches are conducted for a Valid Law Enforcement Purpose while not violating individuals' privacy, civil rights, and civil liberties. This Facial Recognition policy assists the Participating Agency and its personnel in:

- (a) Increasing public safety and improving security.
- (b) Minimizing the threat and risk of injury to the public.
- (c) Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- (d) Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- (e) Protecting the integrity of criminal investigatory and justice system processes.
- (f) Fostering trust by strengthening transparency, oversight, and accountability.
- (g) Making the most effective use of public resources.

600.3 AUTHORIZED USE OF FACIAL RECOGNITION

Access to FRS will be provided only to those individuals from Participating Agencies who are authorized to have access for Valid Law Enforcement Purposes only.

All deployments of the FRS are for official use only and are law enforcement sensitive. All uses of the FRS will be performed on a need-to-know and right-to-know basis per Criminal Offender Record Information (CORI) regulations. Penal Code § 11105, defines who has access to CORI, and Penal Code §§ 11140 through 11144, establish the penalties for the improper use of CORI. Law enforcement agencies are required to abide by the most updated DOJ CORI rules, which can be found on the DOJ's website, as well as the Federal Bureau of Investigation's (FBI) most updated Criminal Justice Information Services (CJIS) Security Policy, which can be found on the FBI website. To the extent these laws, rules and policies may change, Participating Agencies shall take any action necessary to abide by such new laws, rules, policies, standards, or requirements relating to security or privacy of CORI or data within the FRS.

The provisions of this policy support the following authorized uses of Facial Recognition information:

- (a) A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal conduct or activity that threatens any individual or the community.
- (b) An active or ongoing criminal investigation.
- (c) To mitigate an imminent threat to the health or safety of the community.
- (d) To investigate or corroborate tips and leads related to criminal investigations.

Facial Recognition System

- (e) For a person whom an officer reasonably believes is concealing their true identity and has a reasonable suspicion the individual has committed a misdemeanor or felony crime.
- (f) To assist in the identification of a person who lacks the capacity or is otherwise unable to identify themselves, such as a person who is incapacitated, deceased, a danger to themselves or others, or otherwise at-risk, and only as a last resort after other traditional methods of identification have been unsuccessful.

600.4 PROHIBITED USES OF FACIAL RECOGNITION

Facial Recognition shall not be used in the following ways:

- (a) To actively surveil members of the public through any camera or video device unless the person(s) are under an active criminal investigation or the Surveillance is in response to an imminent threat of life;
- (b) On live stream video unless there is an imminent threat to life or at-risk individuals are involved;
- (c) For any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments;
- (d) To prohibit or deter lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute, or as a Probe Image(s) obtained from First Amendment Protected activity;
- (e) For non-criminal purpose, except as defined in subsections IV(c) and (f) above, or purely administrative investigations;
- (f) For harassing and/or intimidating any individual or group;
- (g) For predictive analysis;
- (h) For personal or non-law enforcement purposes. This includes the sharing or utilizing of any PII obtained from the FRS for any purpose beyond the underlying Valid Law Enforcement Purpose;
- (i) To assess immigration status;
- (j) To identify persons pursuing or exercising reproductive rights; or
- (k) Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

600.5 CONSTITUTIONALLY PROTECTED EVENTS, ACTIVITY AND AFFILIATIONS

Facial Recognition must be used in accordance with all federal and state laws, this ILJAO Policy, and all internal Participating Agency policies. The ILJAO and all personnel with access to the FRS will not perform or request Facial Recognition searches about individuals or organizations that will violate any provision of the US Constitution, including the First, Fourth, and Fourteenth Amendments, and based solely on any of the following:

- (a) Their religious, political, or social views or activities.

Facial Recognition System

- (b) Their participation in a particular non-criminal organization.
- (c) Their race, ethnicity, citizenship, place of origin, age, disability, gender, gender identification, sexual orientation, or other protected classification.

600.6 DATABASE AND DATA LIMITATIONS

(a) The Participating Agency will not maintain, utilize, or keep any database to conduct Facial Recognition searches and shall only use the ILJAOC Repository to conduct Facial Recognition searches.

(b) The Participating Agency will only utilize the ILJAOC countywide FRS to conduct Facial Recognition searches.

(c) No databases outside Orange County Automated Biometric Identification System, such as the California driver's license or open-source photo databases, or Automated License Plate Reader images, will be uploaded, accessible, or searchable in the FRS Repository.

(d) ILJAOC does not connect the FRS to any interface that performs live video Surveillance, including Surveillance cameras, drone footage, and body-worn cameras. The FRS will not be configured to conduct Facial Recognition analysis on live or recorded video.

600.7 DOCUMENTATION

Any authorized user from a Participating Agency must Log each access of the FRS. Each agency is required to maintain the Logs for their authorized employees and make them available to the Orange County Sheriff's Department Crime Laboratory (OCCL) for quality control and random auditing purposes. The Logs shall be retained per the Participating Agency's retention schedule.

The Logs must include the following information:

- The name, agency, and contact information of the law enforcement user
- The date and time of access
- Case number
- Probe Images
- The specific information accessed
- The Valid Law Enforcement Purpose
- Number of potential Candidate Images provided by the FRS
- Whether filters or enhancements were utilized, and if so, on which Probe Images.

With any possible match where an Investigative Lead is generated from the Facial Recognition software, the Facial Reviewer or investigator shall write a detailed report on the information they have obtained. The report by the Facial Reviewer must be attached to the criminal investigation report. This must be done even if possible matches are not deemed likely candidate matches or used in the criminal investigation, since the prosecuting agency must be provided with all

Facial Recognition System

investigatory actions taken, whether or not they generate an investigative lead (see Section X below).

It is strongly recommended that Probe and Candidate Images are peer reviewed when feasible for verification by other trained and authorized personnel. Participating Agencies are encouraged to review the quality of the information received from the FRS.

600.8 INVESTIGATIVE SEARCHES AND CANDIDATE IMAGES

- (a) Probe Images will only be used from legally obtained sources.
- (b) Before conducting a Facial Recognition search, Facial Reviewers will review, analyze and evaluate the quality and suitability of a Probe Image, including factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a Probe Image. It is recommended that the results of this process also be documented in the Logs.
- (c) Upon determining the Probe Image(s) are suitable, the Facial Reviewer may process the Probe Image(s) to conduct a Facial Recognition search.
- (d) Investigative searches shall only be conducted by trained Facial Reviewers.
- (e) Only the minimum necessary amount of the Facial Recognition data required for Valid Law Enforcement Purposes may be accessed, copied, downloaded, or shared.
- (f) Candidate Images which result from an investigative search are strictly defined as Investigative Leads. The ILJAOOC considers the results, if any, of a Facial Recognition search to be advisory as an Investigative Lead only. Facial Recognition search results are not regarded as identification of a subject and do not, on their own, establish reasonable suspicion or probable cause without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.
- (g) The following statement shall accompany the most likely Candidate Image(s) and any related records:

"ILJAOOC is providing this information as a result of a Facial Recognition search, utilizing a Repository from criminal livescan records maintained by the Orange County Crime Lab and/or otherwise linked through a Participating Agency with the FRS. This information is provided only as an Investigative Lead and IS 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 lawful investigative resources."

600.9 SHARING FACIAL RECOGNITION INFORMATION

Information obtained from the FRS shall only be shared in accordance with the laws and policies governing CORI and as set forth in section IV above.

Participating Agencies and their members may only disseminate information obtained through the FRS to:

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Facial Recognition System

- Other law enforcement agencies as permitted by this policy.
- A prosecutorial entity for use in a criminal matter to support a prosecution or disclose exculpatory information, in accordance with California statutory law and the California and Federal Constitutions. Any use of the FRS, regardless of the results and whether it results in an investigative lead, shall be disclosed to the prosecuting agency since failure to do may constitute a Brady violation.
- Personnel designated by a California or Federal Court in response to a court order.
- To authorized government or law enforcement agency for the purpose of quality control and auditing.

Facial Recognition Search information shall not be disclosed to unauthorized individuals or for unauthorized purposes. It may not be reproduced for secondary dissemination, transferred to, or shared with any other employing, licensing, or regulatory entity, or in response to a Public Records Act request.

The existence or nonexistence of Facial Recognition information should not be confirmed to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

600.10 TRAINING

Participating Agencies' members who will be users of the Facial Recognition software and serve as Facial Reviewers must attend training prior to accessing the FRS. Investigative searches shall only be conducted by trained Facial Reviewers who are qualified to assess image quality and suitability for Facial Recognition searches and to perform one-to-many and one-to-one face image comparisons.

- Participating Agency personnel accessing the FRS shall have completed training provided by the FBI or ILJAOC, which shall meet the CJIS minimum training criteria for using an FRS.
- Facial Reviewers must attend the Facial Recognition Searches and Advanced Morphological Training through the Facial Recognition software vendor prior to utilizing the FRS.
- All users must also satisfy any additional training requirements for their respective Participating Agency.

All authorized users must also acknowledge the implementation of and their adherence to this Facial Recognition policy. A Participating Agency will provide its authorized users with a printed or electronic copy of this Facial Recognition policy in addition to the Participating Agency's own internal policy and require a written acknowledgment of receipt. All written acknowledgements should be retained by the Participating Agency for reporting purposes as required by law or requested by ILJAOC or OCCL.

Facial Recognition System

600.11 DATA QUALITY ASSURANCE

Original Probe Images will not be altered, changed, or modified in order to protect the integrity of the images. Any enhancements made to a Probe Image will be made on a copy, saved as a separate image, and should be documented in the Logs to indicate what enhancements were made, including the date and time of change.

The integrity of information depends on quality control and correction of recognized errors, which is key to mitigating the potential risk of poor-quality leads or inclusion of individuals as candidates.

Images in an Unsolved Image File should be validated periodically by the contributor to ensure that the criminal investigation remains active and that the image remains relevant to the investigation. If, in accordance with this policy, the contributor has not validated the need to retain the image in the Unsolved Image File, the image shall be immediately purged.

If a Participating Agency identifies malfunctions or deficiencies, including data that may be inaccurate or incomplete, incorrectly merged, out of date, or cannot be verified, it will notify the OCCL Biometric Program Administrator through electronic notification at [REDACTED]. The OCCL will investigate in a timely manner alleged errors, malfunctions or deficiencies, including reviewing the Repository for the data identified by the Participating Agency and edit or remove the data, as appropriate. A record will be kept of all requests for correction and the results of the investigation.

The OCCL will similarly use written or electronic notification to inform all Participating Agencies when information within the Repository is deleted or changed by the OCCL because the information is determined to be inaccurate or incomplete, incorrectly merged, out of date, or cannot be verified.

600.12 GOVERNANCE

The Biometric Program Administrator of the OCCL has primary responsibility for the operation of the ILJAOC's FRS. The OCCL's Director will designate a Biometric Program Administrator who will be responsible for the following:

- Overseeing and administering the FRS to ensure compliance with applicable laws, regulations, standards, and policy.
- Acting as the authorizing official for individual access to Facial Recognition information.
- Ensuring that user accounts and access to use the FRS granted to Participating Agencies are maintained in a current and secure "need-to-know" status.
- Reviewing supporting documentation of FRS requests and results for quality assurance purposes to ensure reliability and accuracy.
- Ensuring that random evaluations of user compliance with system requirements and the Participating Agencies' Facial Recognition policies and applicable law are conducted and documented.

Facial Recognition System

- Confirming, through random audits, that Facial Recognition information is removed in accordance with this policy (see, e.g., Sections XII and XV) and to ensure compliance with applicable laws, regulations, standards, and policy.
- Identifying any potential gaps in the FRS and working with the vendor to make improvements and mitigate potential risks of the FRS process.
- Regularly auditing the documentation reflecting those personnel (including any authorized members from Participating Agencies who may make Facial Recognition search requests) meet all prerequisites stated in this policy prior to being authorized to use the FRS.

OCCL reserves the right to establish the qualifications and number of personnel having access to the FRS and to suspend or withhold service and deny access to any Participating Agency or Participating Agency personnel violating this policy.

600.13 AUDITS

All uses of the FRS and search requests are subject to audit by the DOJ, ILJAOC, and OCCL.

Audits by the OCCL will occur on a monthly basis to ensure lawful access and accuracy of data, and to prevent misuse. The OCCL Biometric Program Administrator will obtain necessary data from Facial Recognition software vendor's support desk to conduct a full and complete audit.

In the event of an audit, the Participating Agency is required to provide the necessary data to the OCCL Biometric Program Administrator, including all Logs and documentation required by this policy and documents that provide appropriate justification for using or requesting a Facial Recognition search. Appropriate justification shall include a situation description and purpose for the search, including a detailed account of circumstances amounting to reasonable suspicion, a case/complaint number, and a file class/crime type, if available.

In addition, Participating Agencies are encouraged conduct quarterly audits of their personnel access privileges to ensure inactive user accounts are disabled.

Participating Agencies' access to the FRS may be terminated by the OCCL if their authorized users violate the terms of this policy. Additionally, authorized users may be subject to additional discipline from their respective agencies for violation of their agency-specific policies. Moreover, other law enforcement agencies, including but not limited to State or Federal agencies, may independently pursue violations of the law.

600.14 SECURITY AND MAINTENANCE

Security Safeguards

Participating Agencies shall implement the security safeguards specified in Attachment A to the Agreement. Any conflict between this policy and the Agreement, or any ambiguity in the terms and conditions of this policy, shall be resolved in favor of the more stringent meaning that complies and is consistent with federal and state laws and regulations. Security safeguards cover any type of

Facial Recognition System

medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used associated or used with the FRS.

The FRS utilizes secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to Facial Recognition information will be allowed only over secure networks. All results produced by Participating Agencies as a result of a Facial Recognition search should be disseminated by secured electronic means.

All Facial Recognition equipment, software, and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

Breach or Security Incident

All individuals with access to the FRS will report a suspected or confirmed Breach or Security Incident to the OCCL Biometric Program Administrator as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a Breach or Security Incident in any medium or form, including paper, oral, and electronic.

Pursuant to the requirements and procedures set forth in Attachment A to the Agreement, Participating Agency shall promptly investigate such Breach or Security Incident. ILJAOC and OCCL shall have the right to participate in the investigation or conduct their own independent investigation, and Participating Agency shall cooperate fully in any such investigation. Following the assessment of a suspected or confirmed Breach or Security Incident and as soon as possible, OCCL, in consultation with Participating Agency, will determine whether it requires notification to an affected agency or individual, in accordance with applicable laws, regulations, policies, and procedures.

Username and Passwords

Access to the FRS will be granted only to authorized users whose positions and job duties require such access and who have successfully complied with the requirements set forth by their Participating Agency. Usernames and passwords to the FRS are not transferable, must not be shared, and must be kept confidential.

If not enforced by the FR system, the Participating Agency must ensure that all users be issued a unique username for accessing Facial Recognition data. The username must be promptly disabled or deleted, or the password changed, upon the transfer or termination of an employee with knowledge of the password.

Passwords must be at least eight characters long and composed of characters from at least three of the following four groups from the standard keyboard:

Facial Recognition System

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation, symbols)

Passwords may not be a dictionary word or proper name, the same as the username, identical to the previous ten (10) passwords, or displayed when entered. Passwords shall expire within a maximum of 90 calendar days. They must not be stored in a readable format on the computer.

Image Removal

Occasionally, images are sealed with a court order or removed for a variety of legitimate reasons (e.g., duplicate, test, inappropriate). Such images will be removed by OCCL during audits or when directed to do so by a valid court order issued by a competent court of law. The OCCL's Biometric Program Administrator will obtain the necessary information from Facial Recognition software vendor's support desk. and notify all Participating Agencies and users of any removed image pursuant to this section that was previously returned as a Candidate Image in an FRS as soon as practical to protect the integrity of any investigations. All court orders regarding images to be sealed or removed should be forwarded to OCCL's Biometric Program Administrator.