# CID 213.00 FACIAL RECOGNITION

| | |
|---|---|
| **TBP:** 7.36 | **CJIS:** |
| **Effective Date:** 7-31-23 | **Review Date:** |
| **Revised Date:** | |
| **Comment(s):** New Policy | |
| **Related Directive(s):** | |
| **Related Form(s):** | |
| **Issued by:** E. Reyes, Police Chief | |

## CID 213.01 PURPOSE

This directive outlines the appropriate applications and restrictions regarding the use of Facial Recognition software / technology as authorized by department policy and state and federal law. The department has established access and use of facial recognition software/technology to support the investigative efforts of law enforcement and public safety agencies. Facial Recognition Technology shall be used only for legitimate law enforcement purposes.

## CID 213.02 POLICY

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face using biometric algorithms contained within a software application. Facial recognition is an investigative tool and WILL NOT be configured to conduct random facial recognition analysis on live or played back recorded video. This technology will provide many opportunities for the enhancement of productivity, increased crime solvability, effectiveness, and increased safety for both citizens and officers. This policy provides personnel with specific guidelines for the collection, access, use, dissemination, retention, purging of images, auditing, and related information applicable to facial recognition.

## CID 213.03 DEFINITIONS

A. **Candidate images** - the possible results of a facial recognition search. When facial recognition software compares a probe image against the images contained in a public repository, the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to, or most likely resemble, the probe image to warrant further analysis.
B. **Facial recognition** - the automated searching for a reference image on an image repository by comparing human facial features of a probe image with the features of images contained in an image repository. A facial recognition search will typically result in one or more most likely candidate images.
C. **Facial recognition administrator -** member designated by the Chief of Police, or designee, to be the point of contact for facial recognition software/technology access, training, and audits.
D. **Facial recognition software/technology** - third party software that uses specific proprietary algorithms to compare human facial features from one specific picture (probe image) to many others that are stored in an image repository to determine most likely candidates for further investigation.
E. **Facial recognition user** - a member who has been approved for access and granted account access by the facial recognition administrator.
F. **Investigative lead** - any information which could potentially aid in the successful resolution of an investigation but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

G. **Probe image** - any uploaded face image used by facial recognition software for comparison with the face images contained within a face image repository.

## CID 213.04 TRAINING

A. Training will be provided to all authorized users of facial recognition software/technology. This training will be arranged and documented by the facial recognition administrator and account access will not be created or provided until training has been completed. (TBP 7.36)
B. Training will cover both the use of facial recognition software/technology and a specific review and acknowledgment of all elements of this policy.

## CID 213.05 AUTHORIZED USER

A. Any and all use of a facial recognition shall be for official law enforcement use only and considered law enforcement sensitive information. The provisions of this policy are provided to support the following authorized uses of facial recognition information.
B. The facial Recognition Administrator shall be appointed by the Chief of Police or his designee. The administrator shall be assigned to the Criminal investigative Division or Administration.
    1. The facial recognition administrator shall maintain a log documenting the following:
        a. Requested query search
        b. Case or Incident number
        c. Individual requesting the search
        d. Results of the image search

## CID 213.06 AUTHORIZED USE OF FACIAL RECOGNITION SYSTEM

A. Any and all use of facial recognition technology shall be for official law enforcement use only and considered law enforcement sensitive information. The provisions of this policy are provided to support the following authorized uses of facial recognition information.
    1. A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
    2. An active or ongoing criminal investigation.
    3. To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (such as incapacitated, deceased, or otherwise at risk).
    4. To investigate and/or corroborate tips and leads.
    5. To assist in the identification of potential witnesses and/or victims of violent crime.
    6. To support law enforcement in critical incident responses
B. The use of facial recognition and access to data requires a legitimate law enforcement purpose. No member may use or authorize the use of or access to facial recognition for any other reason.
C. Probe photos are specifically limited to those obtained lawfully, including those exposed to public view.
D. Any uploaded Probe Image shall be that of an unknown person for the sole purpose of obtaining a possible identification and investigative lead in an official law enforcement investigation. The only exception to this requirement is if the uploading of a known Probe Image may result in additional investigative leads (such as the identification of potential alias', alias social media accounts, etc.).
E. Facial Recognition is an investigative tool and any law enforcement action taken based on a submission to the facial recognition system shall be based on the agency's own identity determination and not solely the results of a facial recognition search. The result of a facial recognition search shall only be considered as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT OR PROBABLE CAUSE FOR ARREST. Any possible connection or involvement of any subject to an investigation must be determined through further investigation and investigative resources.

## CID 213.07 UNAUTHORIZED USE OF FACIAL RECOGNITION SYSTEM

A. The department strictly prohibits access to and use of any facial recognition system, including dissemination of facial recognition search results, for the following purposes:
    1. Non-law enforcement (including but not limited to personal purposes).
    2. Any purpose that violates the U.S. Constitution or laws of the United States, including protections of the First, Fourth, and Fourteenth Amendments.

3. Harassing and /or intimidating of any individual or group.
4. Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

B. Facial recognition software shall not be used to obtain similar images to a subject for the purpose of using them as filler images in a photographic line up.

C. The department **DOES NOT** connect any facial recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras.

EOD