FACIAL RECOGNITION TECHNOLOGY

Section

4.1 **POLICY**: It is the policy of the Miami Police Department to utilize facial recognition technology to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool in developing leads for a criminal or Internal Affairs investigation, detecting and preventing criminal activity, reducing an imminent threat to health or safety, and helping in the identification of deceased persons or persons unable to identify themselves.

4.2 **ORGANIZATION**: This policy shall apply to all sworn and civilian members. The Chief of Police or his/her designee will authorize access to facial recognition platforms.

4.3 DEFINITIONS:

4.3.1 **Probe Photograph**: A still shot/image which is uploaded to the facial recognition software/application.

4.3.2 **Facial recognition technology**: A computer software/application capable of comparing specific physical features of a person depicted in a probe photograph against a database of images of persons identified through other means.

4.3.3 **Facial recognition search result**: An image returned by facial recognition technology that represents a potential investigative lead based on an algorithmic similarity to the submitted image.

4.3.4 **Identification**: The action or process of identifying a person. A positive facial recognition search result alone does not constitute probable cause for arrest.

4.3.4.1 The search result shall be evaluated by the arresting officer or lead investigator and requires investigative follow-up to corroborate the lead by taking such actions including but not limited to: reviewing all relevant reports, conducting interviews, presenting photographic line-ups, and examining all other evidence (i.e. latent prints and DNA). When deciding to arrest based on all factors, the arresting officer or lead investigator shall take into consideration the quality of the probe photograph and the facial recognition search results.

4.3.5 **Commercial facial recognition platform**: Facial recognition software/application that is owned and operated by a private sector entity.

4.3.6 **Face Analysis Comparison & Examination System (F.A.C.E.S.)**: F.A.C.E.S. is a facial recognition database operated by the Pinellas County Sheriff's Office (P.C.S.O.). P.C.S.O. grants access to its database to other law enforcement agencies, including the Miami Police Department.

4.4 **RESPONSIBILITIES**: It is the purpose of this policy to provide members with guidelines and principles for the collection, access, use, and dissemination of images and related information applicable to the use of facial recognition technology. This policy will ensure that all facial recognition technology uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals. All members who make use of facial recognition technology shall familiarize themselves with the limitations of such technology, including algorithmic biases toward affected demographic groups.

4.5 **PROCEDURES**: Facial recognition technology shall only be utilized by authorized Real Time Crime Center (R.T.C.C.) personnel and others authorized by the Chief of Police and his/her designee. **(CALEA 41.3.7a)**

4.5.1 **Authorized uses for commercial facial recognition technology and FACES**: Facial recognition technology shall only be used for the identification of the following: (**CALEA 41.3.7b)**

a) Potential suspects, witnesses, and/or victims in a criminal investigation.

b) Principal officers, witnesses, or other involved person(s) in an Internal Affairs investigation.

c) Persons in need of assistance from law enforcement and who lack the physical, mental, emotional, or cognitive capacity to identify themselves or are otherwise unable to identify themselves.

d) Unidentified deceased persons.

e) Lawfully detained persons refusing to identify themselves or whose identity cannot be established.

4.5.2 **Prohibited use of commercial facial recognition technology and FACES**: Facial recognition technology shall be used for official law enforcement purposes and shall not be used for:

a) Personal use, queries not related to legitimate agency duties, sharing, copying, or the passing of information to unauthorized personnel.

b) Harassing and/or intimidating any individual or group.

c) Facial recognition technology shall not be used to conduct surveillance of persons or groups based solely on their religious, political, or other constitutionally protected activities, their race, ethnicity, gender, sexual orientation, sexual identity, or other constitutionally protected class membership.

d) Facial recognition technology shall not be used to monitor persons in real-time.

e) Any other purpose, access, use, disclosure, or retention that would violate applicable local, state, or federal law or agency policy.

4.5.3 **<u>Process for utilizing all commercial facial recognition platforms from the R.T.C.C.</u>**:

4.5.3.1 Requests for facial recognition services shall be submitted to the Real Time Crime Center via e-mail (rtcc@miami-police.org) with the probe photograph(s) to be reviewed, the incident number (if applicable), the incident type, and any other pertinent information.

4.5.3.2 Authorized R.T.C.C. members will conduct a search of the facial recognition software/application and provide all search results and pertinent information to the requestor. If the investigation requires a case file (e.g., criminal cases assigned to a Criminal Investigations Section investigator), all search results shall be maintained within the investigator's case file. The lead investigator in a criminal investigation will also be cautious in not succumbing to confirmation bias and focusing solely on a "top" search result when attempting to identify a suspect; a reasonable effort must be made to fully investigate other possible suspects identified in search results.

4.5.3.3 The R.T.C.C. shall maintain a log documenting all facial recognition searches performed. The log shall include the date and time the search was performed, incident number (if applicable), incident type, whether the search yielded results, and if there was ultimately a positive identification. Upon determining whether the search result(s) produced a positive identification, the requestor shall notify the R.T.C.C. via e-mail to ensure the log reflects the outcome of the search.

4.5.3.4 The R.T.C.C. may conduct subsequent searches of the probe photograph if an identification is not made during the initial search. All subsequent searches, however, shall be logged, as per Departmental Order 16, Ch. 4.5.4.3.

4.5.4. Process for utilizing Face Analysis Comparison & Examination System (F.A.C.E.S.): Authorized users of F.A.C.E.S. shall comply with all of the site's terms of service.

4.5.5 **<u>Audits</u>**: The R.T.C.C. supervisors responsible for administering facial recognition software account(s) shall conduct a monthly audit to ensure the R.T.C.C. members' compliance with policy. **(CALEA 41.3.7e)**