G.O. Number: 19.6	**Subject:** Biometric Identification Program	
Chapter: 19 Criminal Investigations		Number of Pages: 06
CFA Standard(s): None		**Effective: 06/06/2022**
By Order of Chief of Police: Rene G. Landa Chief of Police		**Revised:** **Status:** New

SECTIONS:

RESCINDS: Any other existing orders in conflict.

PURPOSE: The purpose of this General Order is to establish guidelines and regulations for using biometric identification technology at the South Miami Police Department. A Facial Recognition System (FRS) is to be considered an investigative tool. Information found through an FRS is not probable cause to arrest, and any law enforcement action taken based on a submission to the FRS shall be based on the member's own identity determination and not solely the results of the FRS search.

The South Miami Police Department also uses "Rapid-ID" fingerprint technology in the field. In 2014, mobile Rapid-ID devices were deployed to Law Enforcement Units to identify individuals who are unable or reluctant to properly identify themselves.

SCOPE: All Departmental personnel.

POLICY: It shall be the policy of the South Miami Police Department that the FACESNXT system (as well as any other biometric identification system) will only be utilized for legitimate law enforcement purposes. The use of the FACESNXT system will be in accordance with the Memorandum of Understanding (MOU) between the South Miami Police Department and the Pinellas County Sheriff's Office, the laws of the State of Florida, and of the United States.

19.6.1 DEFINITIONS

A. **AMBIGUOUS RESPONSE**: There was no definitive match using the submitted search prints. More than one possible match was found.

B. **BIOMETRICS**: Distinctive and measurable human characteristics that can be used to identify people apart from demographic data like name and date of birth. Fingerprints and facial features are examples of commonly used biometrics. Since biometrics are unique to individuals, they are more reliable in verifying identity than knowledge based methods.

C. **CANDIDATE LIST**: A rank-ordered list generated from a facial recognition search

D. **ENROLL**: The act of capturing a facial image, creating a template and entering the template into a facial recognition gallery.

E. **FACIAL IDENTIFICATION**: A manual examination of the differences and similarities between facial images or between a live subject and facial images for the purpose of determining if they represent the same person.

F. **FACIAL RECOGNITION**: The automated searching of a facial image (probe) against a known collection resulting in a list of candidates ranked by computer-evaluated similarity score. This is commonly referred to as a one-to-many comparison.

G. **FACIAL VERIFICATION:** The automated comparison of a facial image to a known standalone biometric sample, resulting in a computer-evaluated similarity score. This is commonly referred to as a 1:1 comparison. Also, the process of authenticating a person's asserted identity by comparing two image templates to answer the question, "Are these two images the same person?"

H. **FBI RISC (REPOSITORY FOR INDIVIDUALS OF SPECIAL CONCERNS) SYSTEM**: A searchable database of individuals which includes Wanted Persons, Sexual Offender Registry Subjects, Known or appropriately suspected terrorists, and other persons of special interest.

I. **GALLERY**: The FR system's database, which typically contains all known-person templates.

J. **HIT RESPONSE**: A “match” was found in the FDLE database of criminal records for the fingerprints submitted and the FDLE number is returned.

K. **NO HIT RESPONSE**: No match was found in the FDLE database of criminal records.

L. **PROBE**: The facial image or template searched against the gallery in an automated facial recognition system.

M. **RAPID-ID**: A fingerprint identification system that uses two fingers to search state wide criminal history records and return positive identification along with criminal history information on an individual.

N. **STATE ID NUMBER (ALSO KNOWN AS FDLE NUMBER OR SID NUMBER)**: The sequential number assigned to an individual’s record by the Florida Department of Law Enforcement (FDLE) which allows retrieval of an individual’s complete, statewide criminal record.

O. **STATEWIDE CRIMINAL HISTORY (ALSO KNOWN AS RAP SHEET)** – A listing of an individuals’ arrests, prosecutions, demographic data used by that individual in the criminal justice system and a “flag” when a DNA sample is on file for that individual.

P. **TEMPLATE**: A set of biometric measurement data prepared by an FR system from a facial image.

Q. **WATCHLIST**: A repository of unsolved probe images that is automatically compared to new photos submitted to the criminal arrest repository.

19.6.2 AUTHORIZATION AND MAINTENANCE

A. Only members assigned to the Criminal Investigations Division or those officers authorized by the Chief of Police or his designee will be allowed to access the FACESNXT system.

B. Only members authorized by the Chief of Police or his designee will be permitted to use mobile fingerprint identification devices.

C. The Criminal Investigations Division Supervisor will be responsible for the administration of FRS Program.

D. The system administrator shall audit and manage user accounts and immediately deactivate users who are terminated, retire, or no longer need FRS access.

19.6.3 GENERAL GUIDELINES – USAGE

A. Any usage of the FRS is strictly limited to official law enforcement purposes. All usage is subject to monitoring and audits by the Pinellas County Sheriff’s Office and the South Miami Police Department. If misuse of the FRS by a user(s) is suspected by administrators, the proper chain of command will be notified and further investigation will follow. User accounts may be suspended while investigation of suspected misuse occurs. If misuse of the FRS is substantiated by administrators, the user(s) account will be deactivated until further notice.

B. The FRS may be used in both criminal and non-criminal investigations.

C. Acceptable usage in criminal investigations includes attempting to identify:

1. Individuals suspected of having committed, committing, or about to commit a crime.

2. Decedents, individuals who are otherwise incapacitated, or individuals who are unable to effectively communicate.

3. Individuals who have been lawfully detained that refuse to identify themselves, or their identity is in question.

4. Witnesses of crimes.

5. The victim of a crime.

6. To mitigate an imminent threat to public safety or threat to life.

7. Individuals in furtherance of official law enforcement duties and responsibilities.

8. Below are some examples of non-criminal investigations where the FRS may be effectively used:

    a. Assist with identifying a missing / endangered person who is unable to effectively communicate their identity to law enforcement.
    b. Assist with identifying decedents.
    c. While conducting research for a threat assessment or Risk Protection Order.

D. Authorized users are permitted to conduct searches using the FRS for functionality testing and training. These searches must be conducted only using authorized probe images such as those of the authorized user conducting the testing or training.

E. Members who are authorized to use the FRS for investigations may access the software through their assigned agency computer or smartphone. Authorized members may utilize their agency assigned smartphone to access the mobile FR application for probe collection and FR search.

F. All facial recognition investigations will be conducted with the safety of all officers and person(s) being photographed as the paramount concern.

G. Members will bring any problems with the FRS to the immediate attention of a supervisor.

19.6.4 RESTRICTIONS

A. The FRS will not be used to assist in identifying persons engaged in lawful peaceful assemblies or protests unless such person(s) are directly related to a criminal investigation.

B. The FRS will not be used for real-time tracking or monitoring of individuals.

C. Individuals will not be physically detained for the purpose of taking a photograph for facial recognition. Officers should ask for consent; this does not preclude an officer taking the photograph of a person in a public place provided the officer has not hindered the movement of the person.

D. Physical force shall not be used for the purpose of taking a photograph.

E. An individual in public shall not be stopped or told to pose for a photograph when it is not being done for a law enforcement investigation, i.e., a person in a motor vehicle shall not be required to roll down tinted windows or uncover their face just for the purpose of taking their photograph.

19.6.5 RAPID-ID FINGERPRINT TECHNOLOGY

A. Authorized SMPD members may utilize handheld devices for investigations requiring fingerprint identification or fingerprint verification of a subject's identity. Fingerprint identification is performed using portable fingerprint capture devices and the dedicated software application on the computer "paired" with the capture device.

1. Search results are returned to both the handheld device and the laptop application for review.

2. Results are either a "Hit", a "No Hit" or an "Ambiguous" response.

3. In the case of "No Hit" or "Ambiguous" response, fingers of the other hand may be captured and searched to confirm initial result.

19.6.6 TRAINING

A. All users are required to complete the online training modules and pass quiz questions with a score of 80% or better prior to gaining access to FACESNXT. Training documentation and videos will be available to users if needed for further review. These can be found after logging into FACESNXT and clicking the Help button (question mark icon) from the Home page.

B. Training in the use of "Rapid-ID" mobile fingerprint identification devices is provided when equipment is issued and software is installed on a member's assigned computer.