MICHIGAN STATE POLICE
STATEWIDE NETWORK OF AGENCY PHOTOS (SNAP)
ACCEPTABLE USE POLICY

I. Purpose

The purpose of this policy is to establish procedures for acceptable use of the images, information, and tools within the Statewide Network of Agency Photos (SNAP) application.

II. Definitions

A. "Biometric data" is data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and facial recognition data.

B. "Facial recognition (FR)" is the automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity.

C. "Highly Restricted Personal Information" is an individual's photograph or image, social security number, digitized signature, medical and disability information.

D. "Mobile Facial Recognition (Mobile FR)" is the process of conducting an automated FR search in a mobile environment.

E. "Personally Identifiable Information (PII)" is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

F. "Statewide Network of Agency Photos (SNAP)" is a computer application managed by the SNAP Unit, deployed through the Michigan Criminal Justice Information Network (MiCJIN) Portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

G. "User" is an individual who is authorized to access the SNAP application and whose agency is approved by the Michigan Department of State Police (MSP) to utilize the SNAP.

III. Disclosure and Use of Information

A. All technology associated with the SNAP, including all related hardware and software support, is bound by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy, particularly Policy Area 13, and the Michigan CJIS Security Addendum.

B. The information within the SNAP databases is considered highly restricted personal information and PII which may only be transmitted, accessed, used, disseminated, and disposed of in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to, the most recent federal CJIS Security Policy, the Michigan CJIS Security Addendum, the CJIS

Policy Council Act (1974 PA 163), MCL 28.211-28.216, and the most current CJIS Administrative Rules.

C. Improper access, use, or dissemination of highly restricted personal information or PII obtained from the use of the SNAP may result in criminal penalties and/or administrative sanctions. Criminal violations include, but are not limited to, those found in MCL 28.214 and MCL 257.903.

IV. Michigan Department of State (MDOS) Images

The SOS database contains a copy of images captured by the MDOS. MDOS images are considered highly restricted personal information that may be used by a federal, state, or local governmental agency for a law enforcement purpose authorized by law.

A. When possible, other photographs (e.g., criminal mug shots, personal photographs) should be used rather than MDOS images.

B. When releasing MDOS images to the public for law enforcement purposes (e.g., wanted posters, flyers), all information identifying the image as an MDOS image shall be removed.

C. MDOS images shall not be used for candidates other than the primary suspect in a photo lineup. An MDOS image of the primary suspect may be used as part of a photo lineup. Photo lineups shall not include individuals aged 17 or under at the time of image capture. MCL 712A.32 provides the court with the power to order a juvenile to appear for identification by another person.

V. Criminal Mug Shots and Scar, Mark, and Tattoo (SMT) Images

A. Policy regarding the public release of criminal mug shot images may vary by agency. Prior to releasing an image to the public, approval shall be received from the originating agency, except when required under the Freedom of Information Act.

B. Prior to releasing an image to the public, the User shall ensure that the individual's criminal history reflects a corresponding record associated with the image and the image is not exempt from public release.

C. Criminal mug shot images may be used as the primary suspect and all other candidates in a photo lineup. Photo lineups shall not include individuals 17 or under at the time of image capture. MCL 712A.32 provides the court with the power to order a juvenile to appear for identification by another person.

VI. Facial Recognition (FR)

A. FR is not a form of positive identification and results shall be considered an investigative lead only. The lead must be further investigated.

B. FR shall only be used for a law enforcement purpose authorized by law.

C. It is recommended per the Facial Identification Scientific Working Group (FISWG) and the Organization of Scientific Area Committees (OSAC) for Forensic Science, only trained facial examiners should conduct FR searches. Training provided by the SNAP Unit on how to use and access the SNAP application does not qualify a user as a trained facial examiner.

D. MSP members shall only use department-issued devices for Mobile FR. Local agencies are responsible for establishing their own policy regarding the use of personal devices for Mobile FR in accordance with the FBI CJIS Security Policy.

E. Mobile FR shall only be used during the course of a User's lawful duties and one of the following circumstances exists:

   i. Mobile FR may be used with consent of an individual:

      1. The individual may withdraw consent at any time. If consent is withdrawn, and the use of Mobile FR is solely based upon consent, use of Mobile FR is not authorized, and its use must stop immediately.

   ii. Mobile FR may be used without consent of an individual if one of the following circumstances exists:

      1. The User has probable cause to believe the individual has committed a crime for which the collection of biometric data is allowable under MCL 28.243.

      2. The individual is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death, and immediate identification is needed to assist the User in performance of his or her lawful duties.

      3. Pursuant to a valid court order.

F. Users shall indicate the purpose for utilizing Mobile FR.

G. Mobile FR users are configured to receive MDOS images in Mobile FR results, and shall adhere to the following:

   i. Pre-existing images, including, but not limited to, social media photos and surveillance stills, shall not be submitted through Mobile FR. Failure to comply will result in the User's access to MDOS images in Mobile FR results being terminated.

   ii. Users agree to complete additional training and testing as provided by the MSP Digital Analysis and Identification Section in order to maintain access to Mobile FR. This will require written acknowledgement of understanding and agreement to adhere to the SNAP Acceptable Use Policy.

VII. WATCHLIST

A. Images uploaded into the WATCHLIST must be legally obtained and the User shall have a legal right to use the image for law enforcement purposes.

B. Once the individual has been located, the User shall contact the SNAP Unit to request removal of the image from the WATCHLIST.

VIII. Auditing and Penalties for Misuse

A. All FR use is subject to audit by the MSP SNAP Unit. In the event of an audit, the User will be required to provide appropriate justification for the use of FR. Appropriate justification may include a case/complaint number and file class/crime type, if available, or a situation description

and purpose for the search. For searches conducted on behalf of another individual, the name and rank/job title of other individual requesting the search shall also be included.

B. All audit findings and administrative sanctions imposed are at the sole discretion of the MSP. Penalties that may be imposed include, but are not limited to, termination of a User's access to SNAP and termination of agency-wide access to SNAP.