USE OF FACIAL RECOGNITION TECHNOLOGY

1. **PURPOSE**

   The purpose of this policy is to provide guidance on the use of facial recognition technology and to establish procedures for its proper use and accountability. Facial recognition technology involves a computer system's automated search of a human face using biometric algorithms to identify similar facial images within a database (one-to-many). This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. <Insert Agency name> uses facial recognition technologies to support the investigative efforts of law enforcement and public safety agencies in Maryland.

2. **SCOPE**

   This policy applies to all personnel that use facial recognition technology. Facial recognition technology is defined under Maryland law as a computer program, service, or any other technology that analyzes facial features and is used by or at the direction of a law enforcement agency for the identification, verification, or persistent tracking of individuals in still or video images for use in criminal investigations.

   Facial recognition technology does not include technology used only for the analysis of facial features to grant or deny access to an electronic device or that uses an automated or semi-automated process only for the purpose of redacting a recording or an image for release or disclosure outside of a law enforcement agency to protect the privacy of a subject depicted in the recording or image if the process does not generate or result in the retention of any biometric data or surveillance information.

3. **POLICY**

   A. The policy of <insert agency> is to utilize facial recognition technology in a manner that is consistent with authorized purposes to protect the community as well as civil rights and civil liberties. Images provided by facial recognition technology will be evaluated by an employee of the agency authorized to use facial recognition technology in the course of an investigation. Facial recognition technology results provided by the authorized user are investigative leads and cannot be considered positive identification without further investigation. Personnel will comply with all requirements of Maryland Criminal Procedure Section 2-501 et seq. “Facial Recognition Technology.”

   B. <Agency representative-title> is responsible for overseeing and administrating the use of facial recognition technology in compliance with Maryland law, local law, regulations and policies.

C. **Approved Uses of Facial Recognition Technology**

1. Facial recognition technology may only be used by trained personnel designated by the <agency representative-title>, or their designee for the following circumstances:

    a. To assist in the investigation of the following enumerated crimes or the following circumstances:

        1. a crime of violence as defined in Section 14-101 of the Criminal Law Article;
        2. a human trafficking offense under Title 3, subtitle 11 of the Criminal Law Article;
        3. first or second-degree child abuse under Section 3-601 of the Criminal Law Article;
        4. child pornography offense under Section 11-207 of the Criminal Law Article;
        5. a hate crime under 10-304 of the Criminal Law Article;
        6. a weapon crime under Section 4-102, 4-103, 4-203(a)(1)(iii) or (iv), 4-204, or 4-303(a)(2) of the Criminal Law Article;
        7. a weapon crime under Section 5-138, 5-140, 5-141, 5-207(c)(16), 5-406(a)(3), or 5-703(a) of the Public Safety Article;
        8. aggravated cruelty to animals under Section 10-606 or 10-607 of the Criminal Law Article;
        9. importation of fentanyl or a fentanyl analogue under Section 5-614(A)(1)(xii) of the Criminal Law Article;
        10. stalking under Section 3-802 of the Criminal Law Article;
        11. a criminal act involving circumstances presenting a substantial and ongoing threat to public safety or national security;
        12. a crime under the laws of another state substantially equivalent to a crime listed in items 1 through 10 of this item involving a fugitive from justice charged with a crime in that state;
        13. identifying a missing or deceased person or a person who is incapacitated and unable to otherwise provide the person's own identity;
        14. redacting a recording or an image for release or disclosure to protect the privacy of an individual depicted in a recording or an image;
        15. forensic analysis of electronic media seized by law enforcement in relation to a specific investigation if the person identified in the electronic media is not the subject of criminal charges resulting from the forensic analysis;
        16. enhancing security systems for preventing unauthorized access to information, goods, materials, areas, or other properties under the custody or care of a law enforcement agency;
        17. conducting otherwise legitimate activity unrelated to a criminal investigation.

D. **Prohibited Uses of Facial Recognition Technology**

1. <Insert Agency name> respects the constitutional rights of individuals and will not utilize facial recognition technology on a subject who is engaged in activity protected under the United States Constitution, the Maryland Constitution, or the Maryland Declaration of Rights, unless there is reasonable suspicion to believe that the individual has committed, is in the process of committing, or is about to commit a crime or who is not intended to be identified.
2. Facial recognition technology may not be utilized based solely on:
    a. personal interest not related to legitimate duties or objectives of the law enforcement agency;
    b. an individual's political or social beliefs;
    c. an individual's participation in lawful activities; or
    d. an individual's race, color, religious beliefs, sexual orientation, gender, disability, national origin, or status as being homeless.
3. Pursuant to Maryland General Provisions, Section 4-320(g)(2), a person receiving personal information under subsection (d), (e), or (f) may not disclose the personal information to a federal agent or federal agency for the purpose of federal immigration enforcement unless the person is presented with a valid warrant issued by a federal court or a court of this State.
4. Personnel are prohibited from using facial recognition technology to analyze a sketch or manually produced image.
5. Personnel may not disclose to a witness in a criminal investigation, prior to the witness participating in a live identification or photo array, that a particular suspect or image of a suspect was identified using facial recognition technology.
6. Facial recognition technology may not be used for the purpose of live or real time identification of an image or recording.

E. Facial Recognition Searches

1. Authorized users shall only utilize databases or systems for facial recognition searches that comply with Maryland law.
2. Personnel designated to utilize facial recognition technology will be trained in face comparison and identification as well as attend annual bias training in accordance with Maryland law.
3. All facial recognition leads shall be independently verified by an individual authorized to use facial recognition technology.
4. Self-initiated facial recognition searches on crime alert bulletins from other agencies may be conducted by personnel trained and approved in the use of facial recognition.
5. Facial recognition technology may not be knowingly used to assist in a manner that contradicts Maryland law or agency policy.

F. Process for Requesting Facial Recognition Technology Assistance

1. <Insert Agency procedures>

G. Facial Recognition Technology Results

1. All results obtained by facial recognition technology will be provided to the requester in writing and contain the following information:

   a. facial recognition technology was utilized to develop the provided investigative lead;

   b. information contained within the investigative lead is not a positive identification of any individual;

   c. results generated by facial recognition technology may only be considered or introduced as evidence in connection with a criminal proceeding for the purpose of establishing probable cause or positive identification in connection with the issuance of a warrant or at a preliminary hearing; however, facial recognition results may not be the sole basis to establish probable cause and requires support by additional, independently obtained evidence. Additionally, facial recognition technology results may not be introduced as evidence in a criminal trial or in an adjudicatory hearing held under Section 3-8A-18 of the Courts Article.

   d. a summary indicating:

      1. the name of each facial recognition system used;

      2. a description and the name of the databases searched;

      3. any results generated that led to further investigative action from each database or system used.

H. **Audits and Maintenance of Records**

1. Annually, prior to October 1 of each year, the use of facial recognition technology will be audited by the <Insert Agency designee>.

2. The audit will be conducted to determine compliance with Maryland law and policy, to include:

   a. ensuring discovery reports contain the names of each facial recognition system used, a description and the names of the databases searched, and results generated from the use of the facial recognition technology that led to further investigative action;

   b. ensuring personnel designated to utilize facial recognition technology have attended the required training in accordance with Maryland law and agency policy;

   c. ensuring that all required annual reports are completed, and that required disclosures are posted on the agency website;

d. ensuring that an annual report for the prior year's use of facial recognition technology is published, and submitted to the Governor's Office of Crime Prevention and Policy.

3. The results of the audit shall be maintained by <Insert Agency designee> for at least 3 years.

4. The results of the audit and any reference materials shall be disclosed if requested by an entity referenced under Maryland law.

I. **Reporting Requirements**

1. On or before February 1 each year, <Insert Agency designee> shall publish a report that discloses information on the use of facial recognition technology for the prior calendar year, including:

   a. the name of each facial recognition system/database used;

   b. the number of facial recognition searches used for each system;

   c. the justification (i.e. the specific enumerated crime or other authorized use) for each search;

   d. the total number of possible matches that led to further investigative action for each search, including the age, race, and gender of the individuals connected to the possible matches returned, if the information is available from the government records searched;

   e. any and all data breaches or unauthorized uses of facial recognition technology under the agency’s control.

2. A copy of the report shall be sent to the Governor’s Office of Crime Prevention and Policy prior to May 1 of each year.

3. This policy serves as the use and data management policy as required by Maryland law.

4. <Insert Agency name> shall post on its website:

   a. a copy of this policy;

   b. the name of its facial recognition system;

   c. the names of all nongovernmental facial recognition systems utilized, and;

   d. the names and description of all nongovernmental databases searched.