

STATE OF UTAH Utah Statewide Information & Analysis Center POLICY AND PROCEDURES	REF. Facial Recognition 1-12-1	PAGE 1 of 2
	EFFECTIVE DATE 10-31-11	REVISION DATE 00-00-00
SUBJECT: Facial Recognition System		

I. Purpose

To establish the Utah Statewide Information & Analysis Center (SIAC) policy regarding the use of the Facial Recognition System, in providing lead material for the identification of suspects in criminal investigations.

II. Definitions

- A. **SIAC:** Utah’s Statewide Information & Analysis Center.
- B. **Submission/Request:** A request received by the SIAC to utilize Facial Recognition in support of a criminal investigation. Submissions will not contain original evidence.
- C. **Enrolled Image:** Any image contained in the Facial Recognition System such as; booking, prison, Utah drivers’ license, and Utah ID photos that are used to compare to a submission or request.

III. Policy

- A. **PRIVACY AND SECURITY** - Use of Facial Recognition as an investigative tool will fall under the same guidelines (UCA 53-10-104 (9), (10) and CFR 28 part 23) as all SIAC intelligence databases as well as under the SIAC Privacy Policy.
 - 1. All Utah Drivers licenses, ID photos, and all other photos contained and enrolled in the Facial Recognition database will remain in the custody and control of the Utah Department of Public Safety.
 - 2. Images received in a request or submission will not be stored as enrolled images within the Facial Recognition System.
 - 3. Images enrolled in the Facial Recognition System will not be released to anyone other than law enforcement and only in conjunction with an authorized criminal investigation.
 - 4. Only requests or submissions received in accordance with ‘Proper Use’ guidelines will qualify for use of the Facial Recognition System.
- B. **PROPER USE** - The Facial Recognition System is designed to be used in conjunction with, and as a supplement to traditional investigative procedures.
 - 1. Facial Recognition requests can only be submitted in conjunction with an official law enforcement investigation.
 - 2. Law enforcement officers/agencies must provide information demonstrating an active investigation is ongoing.

3. A case/department/intelligence report number and type of criminal investigation are required with every request for a facial recognition investigation.
4. The results of a submission are for lead purposes only, and any further confirmation as to the identity of the submission shall be the sole responsibility of the requestor.
5. Results and images of all submissions will be disseminated to the requesting agency and only the original request and case will be maintained on file.

C. RECORD KEEPING

1. A Facial Recognition request and any results of the inquiry will be maintained in accordance with appropriate current SIAC document maintenance and destruction policies.
2. A searchable, computerized Facial Recognition Database will house a record of all request and results. The database will automatically set a purge date for each case file.
3. Facial Recognition searches that result in a positive investigative outcome (i.e. identification, location, arrest, conviction, recovery, etc.) will also be maintained within the Facial Recognition Database.

D. DISSEMINATION

1. All images and results from the facial recognition system must be approved by a Supervisor prior to dissemination.
2. All results produced by the SIAC as a result of a Facial Recognition search are disseminated by secured electronic means (such as an official government email address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.
3. Media disseminations will occur only with SIAC management and requestor authority.

E. GENERAL AUTHORITY

1. Any submission or request not addressed in this Policy and Procedure must be approved by SIAC executive management.
3. All policies and procedures regarding submission / dissemination will be in accordance with SIAC policy.