County of Santa Clara
Office of the District Attorney's Crime Laboratory
Surveillance Use Policy

Access Card and Biometric Fingerprint Systems

1. Purpose

The Santa Clara County District Attorney's (DA) Crime Laboratory, situated at 250 West Hedding Street, San Jose, is a secure building and site that is accessible to only authorized personnel via a Lenel United Technologies electronic ID badge/access card system and high-security Medeco metal key system. This Surveillance Use Policy supplements the Countywide Surveillance Use Policy for Facility Access Control Technology, since this Surveillance Use Policy contains certain information that is specific to the Crime Laboratory.

Facility access control levels shall be determined by the Crime Laboratory Director based on specific Crime Laboratory assignments that require access into specified areas within the building. Sensitive areas within the building, including rooms where evidence or firearms are stored, shall be accessible via a combination of a Lenel electronic access card and a BioScrypt biometric fingerprint reader. This additional level of security ensures that access is granted by the Crime Laboratory Director to only the individual to whom the access card is issued.

2. Authorized and Prohibited Uses

The electronic access card system and biometric fingerprint system, and the data within those systems, shall be used only for the following limited County and DA Crime Lab business purposes:

- To access the Crime Laboratory and parts of the building for DA Crime Lab business purposes, as specified below;
- To audit or monitor access to the Crime Laboratory and parts of the building, including investigations relating to unauthorized or inappropriate access or use of the system;
- To enhance safety, security, and the preservation of evidence within the Crime Laboratory.

Crime Laboratory employees (including the Crime Laboratory Director, Assistant Crime Laboratory Director, Supervising Criminalists, Criminalists, Criminal Investigators, Property/Evidence Technicians, Storekeeper, and administrative office staff) shall be authorized to use the Crime Laboratory's electronic access card system, subject to the ultimate approval of the Crime Laboratory Director or the Director's written designee.

Other County employees who conduct business at the Crime Laboratory facility (including the District Attorney, Chief Assistant District Attorney, Special Assistant District Attorney/Laboratory Liaison, janitorial staff, and members of the County's Facilities and Fleet department) shall also be authorized to use the Crime Laboratory's electronic access card system at a lower access level, subject to the ultimate approval of the Crime Laboratory Director or the Director's written designee.

Crime Laboratory employees whose duties require them to access evidence and/or firearms shall also be authorized to use the biometric fingerprint system, subject to the ultimate approval of the Crime Laboratory Director or the Director's written designee.

Authorized users shall be issued an access card with a photograph and specific County information on it. When biometric access is authorized, a record of the user's fingerprint shall be kept by the Laboratory for identification purposes.

Unauthorized users shall not use the access-card system, the biometric fingerprint system or the data from the systems. No one shall use those systems to access a part of the building or evidence/firearms within the building for any purpose other than the performance of their required County job duties. It shall be prohibited for any individual to use those systems or their data for personal or other purposes or to access areas, evidence, or firearms the person is not specifically authorized to access.

3. Data Collection

ID badge/access card holder information, including a single fingerprint of each employee's finger, and a record of every ID badge/access card and biometric fingerprint transaction shall be recorded and stored by the County through its Facilities and Fleet Department (FAF).

4. Data Access

The data collected by the ID badge/access card and biometric fingerprint systems for the Crime Laboratory shall be accessible by only authorized members of FAF, the Crime Laboratory's Director, and the Crime Laboratory's Facility Manager, via a secure, password-protected computer.

5. Data Protection

System data shall be maintained, controlled, operated, and administered by FAF's Information Technology Unit, unless the FAF Director designates in writing another specific person or unit to do so. Data access shall be through only secure means. See the Countywide Surveillance Use Policy for Facility Access Control Technology, which addresses data-protection for technology within FAF's control, including the secure central electronic card access system.

6. Data Retention

See the Countywide Surveillance Use Policy for Facility Access Control Technology, which addresses data retention.

7. Public Access

See the Countywide Surveillance Use Policy for Facility Access Control Technology, which addresses public access. Generally, there is no direct public access to the information stored in the County's central electronic card access system. If a California Public Records Act request, subpoena, or court order is issued for access card or biometric fingerprint system data, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Office of the County Counsel as needed.

8. Third-Party Data-Sharing

See the Countywide Surveillance Use Policy for Facility Access Control Technology, which addresses third-party data-sharing. It shall be permissible for data relating to Crime Laboratory access and underlying biometric fingerprint data relating to the system to be shared with law enforcement agencies, County-retained investigative personnel, or other investigative personnel in connection with a specific administrative, civil, or criminal investigation or action; and only with the written consent of the FAF Director or Crime Laboratory Director or their written designees. In addition, employee-access levels shall be shared with the Crime Laboratory's accrediting body, the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) during annual assessment, to satisfy an accreditation requirement pertaining to laboratory security and restricted access.

9. Training

Authorized users shall be provided on-the-job training by the Facility Manager or written designee regarding the use of the access card and biometric fingerprint systems within the Crime Laboratory. All Crime Laboratory employees shall be given a copy of this Surveillance Use Policy.

10. Oversight

FAF shall oversee and control the Crime Laboratory's access card and biometric fingerprint systems. The Crime Laboratory's Facility Manager shall have administrative authority to set and change Crime Laboratory employees' access levels, with written approval by the Crime Laboratory Director. The Facility Manager shall be the only Crime Laboratory employee with access to logs of all system transactions via a "Reports" feature. These logs shall not be altered or deleted by the Facility Manager. See the Countywide Surveillance Use Policy for Facility Access Control Technology for additional oversight information.

Approved as to Form and Legality

Rob Coelho 10/29/18

Rob Coelho, Office of the County Counsel