County of Santa Clara Roads and Airports Department Surveillance Use Policy

Facility Security Camera Systems

1. Purpose

To enhance the security and protections of the Department's employees, facilities, and the public, the Roads & Airport Department shall use security camera systems to assess and record Department facilities and properties, including the Airport Department and Airport facilities, and the Roads Department's East Yard, South Yard, and West Yard.

The Department currently uses various makes and models of security cameras:

- Avertx NV160 system;
- Pelco Analog Model Number CC3710H-6
- Axis P3344 Cameras

2. Authorized and Prohibited Uses

Facility security cameras shall be used only to provide live video feeds for gate control at road-maintenance yards to grant or deny access to uncredentialed individuals; to control and record access to various Roads & Airport Department facilities; and to assist staff to assess and investigate behavior or activity that reasonably appears to be unauthorized, in violation of Department or County policy, illegal, or in furtherance of illegal activity. All Department facilities with operating security cameras shall have easily observable signs disclosing that video surveillance or video monitoring is occurring.

The Department Director, Deputy Directors, Director of Airports, Assistant Director of Airports, or other County personnel designated in writing by the Department Director, shall have the authority to review real-time footage and recorded footage to observe data captured on the security cameras; and to use that data for bona fide administrative investigations, as well as to respond to law enforcement inquiries or provide local law enforcement authorities with images or video clips of specific behavior or activity that reasonably appears to be unauthorized, in violation of Department or County policy, illegal, or in furtherance of illegal activity.

The security camera systems and resulting images and video shall be used for County business purposes only, and not for personal purposes, non-County-business purposes, or illegal purposes. The security camera systems and resulting images and video shall be used in a legal manner; and shall not be used to harass, intimidate, or discriminate against any individual or group.

The security camera systems shall not be used in areas where there is a reasonable expectation of privacy, such as restrooms, changing rooms, lactation accommodation rooms, or other areas

where an individual would reasonably expect not to be recorded despite signage on-site indicating the presence of video monitoring.

3. Data Collection

The security camera systems shall collect, record, and archive video and images of Department facilities and properties at various locations, which may include individuals and activities occurring there. The gate-control systems at the County airports shall record individual users' access to secure areas of the airports.

4. Data Access

Video footage shall be stored on secure video recorders and/or servers. Data access shall be controlled by a designated system user, and shall be restricted to the following management and staff:

- the Department's Executive Managers;
- in the case of airport-related systems, to the Director and Assistant Director of County Airports;
- County staff members designated in writing by the Department's Executive Managers, or the Director or Assistant Director of the County Airports, as applicable, as having a County business need to access the data, in compliance with this Policy;
- Other County personnel designated in writing by the Department's Executive Managers, or the Director or Assistant Director of the County Airports, as applicable, if they determine that access is reasonably necessary for a specific criminal, civil, or administrative investigation or action.

Efforts shall be made to keep the total number of designees with access to the data as low as possible within the constraints of this Policy.

5. Data Protection

Live video feeds shall minimize access by the public and those not authorized to access the data. Servers where recorded data is stored shall be in a secure location and shall have other data-security protections, such as passwords, to limit access to those authorized to access the data.

Archived data from Roads Department facilities shall be stored in password-protected digital repositories located in locked facilities. The servers shall be encrypted and shall require a password or other security credentials for access to occur. Archived data from Airports Department facilities shall be stored in password-protected digital repositories in a locked location.

//

//

6. Data Retention

The Department shall maintain/retain video data for no more than 30 days before the data is recorded over, unless required by law to be retained for a longer time or approved by an executive manager (for Roads data) or the Director of County Airports or written designee (for Airport data) to be retained for a longer time relating to a specific administrative, civil, or criminal investigation or action. It shall be permissible for copies of video data for a specific administrative, civil, or criminal investigation or action to be kept for at least the duration of the investigation or action. Video data that is retained by the Department for these purposes shall be destroyed no later than one year after the administrative/disciplinary or criminal investigation or proceeding has concluded, unless it is retained for training purposes or the law or County policy require a longer retention.

7. Public Access

Any public requests for recorded video images shall be submitted to the Department's CPRA (California Public Records Act) Coordinator for handling. Reasonable efforts shall be made to preserve the data requested until the request has been processed.

If a CPRA request, subpoena, or court order is issued for recorded images or video, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law. Department personnel shall consult with the Office of the County Counsel to ensure legal compliance.

8. Third-Party Data-Sharing

Third party data sharing shall be limited to the following:

- Specific files or data shall be provided to law enforcement representatives, the Federal Aviation Administration (FAA), the Flight Standards District Office (FSDO), or the National Transportation Safety Board (NTSB) if the Department's Executive Managers or Airports Department managers believe that the data may show behavior or activity that reasonably appears to be unauthorized, illegal, or in furtherance of illegal activity; or for the purposes of investigating accidents or incidents on County property;
- Law enforcement agencies, County-retained investigative personnel, or other investigative personnel, but data sharing under this bullet-point shall be permissible with those agencies/individuals only in connection with a specific administrative, civil, or criminal investigation or action; and only with the written consent of the Department's Executive Managers, or in the case of airport-related systems, to the Director and Assistant Director of County Airports;
- Parties in civil litigation involving the County, in response to a subpoena or civil discovery;
- County Personnel Board, arbitrator, or Court regarding a county administrative action or litigation;

- Other third parties, pursuant to a Court Order.

Data may be requested by an employee or an employee representative regarding a specific claim, allegation, or action against the employee; or law enforcement; or a third party seeking compliance with a court order or subpoena or relative to an accident or incident. Each request shall be reviewed by a CPRA Coordinator, Department Executive Manager, or Airports Department manager, who shall seek assistance as appropriate from the Office of the County Counsel and the Labor Relations Department.

9. Training

Department staff members who are granted access to the security camera systems or their data shall be appropriately trained, and shall be made aware of this Policy.

10. Oversight

The Department's Executive Managers and the Director/Assistant Director of County Airports shall oversee compliance with this Policy. Internal requests for data from any of the facility security camera systems shall be submitted to an Executive Manager (or the Director of County Airports in the case of airport-related systems) and shall be logged and filed by Roads Administration. At the end of each fiscal year, the Department's Deputy Director – Administration or written designee shall audit all logs for misuse, including failure to comply with this Policy.

Any employee found to have violated this Policy shall be subject to possible discipline. Alleged violations of this Policy shall be reviewed by the Department Head and written designee(s) with the assistance of the Labor Relations Department and the Office of the County Counsel.

Approved as to Form and Legality

Rob Coelho 12/6/19

Rob Coelho
Office of the County Counsel