

County of Santa Clara Countywide Surveillance Use Policy

Video Security Cameras

1. Purpose

County departments conduct operations and provide services at numerous County facilities throughout Santa Clara County. The County monitors many of these facilities through the use of video security cameras that collect and record video footage of activity in and around County facilities. The purposes for the video security cameras shall be for public safety and the identification, assessment, investigation, and reporting of behavior or activity that legitimately appears to be: in violation of Department or County rule, policy, or reasonable expectation; illegal; or in furtherance of illegal activity.

This Policy shall apply to a County department's use of video security cameras, unless a more specific, Board-approved Surveillance Use Policy for security cameras applies.

This Policy shall not apply to the use of video security cameras that record audio or to video security cameras that record only a private workspace, such as an individual employee's office or cubicle; such cameras require a separate Board-approved Surveillance Use Policy. This Policy shall not preclude a department from developing, and the Board from approving, site- or department-specific security camera use policies.

This Policy shall supersede the following Board-approved Surveillance Use Policies:

1. Communications Department – Video Cameras Used for Facility Security (Approved 10/30/2018)
2. Consumer & Environmental Protection Agency – Vector Control System Campus Security Cameras (Approved 10/16/2018)
3. Department of Child Support Services – ExacqVision Video Security System (Approved 10/30/2018)
4. Finance Agency – Security Cameras (Approved 10/30/2018)
5. Multi-Departmental County Facilities Located at the West Tasman Campus, San Jose – Security Cameras (Approved 11/03/2020)
6. Multi-Departmental Facility Oakland Road Warehouse – Security Cameras (Approved 11/03/2020)
7. Office of the Assessor – Video Cameras in the Assessor's Office (Approved 12/17/2019)
8. Office of the Medical Examiner-Coroner – Video Surveillance Cameras for Building Security (Approved 06/23/2020)
9. Santa Clara Valley Health and Hospital System – Security Video Cameras at SCVHHS Facilities (Approved 10/22/2019)
10. Social Services Agency – Video Security Cameras (Approved 12/17/2019)
11. Technology Services and Solutions – Security Cameras (Approved 10/30/2018)

12. Technology Services and Solutions – Security Cameras and Collected Data
within the Facilities and Fleet Department (Approved 10/16/2018)

2. Authorized & Prohibited Uses

The County-owned and/or County-used video security cameras shall be used to monitor activity as described in Section 1 of this Policy. To establish appropriate privacy expectations, dedicated signage notifying the public, employees, and others of video monitoring and recording shall be placed conspicuously at or near the main entrances of County-operated facilities where video security cameras are deployed by one or more County departments. Such signage shall be posted before each camera system (“System”) is activated.

Each System covered by this Policy, and resulting images and video, shall be used for County business purposes only, and only in support of safety and security purposes, investigative purposes, or training purposes. Safety and security purposes and investigative purposes shall include public safety and the identification, assessment, investigation, and reporting of behavior or activity that legitimately appears to be: in violation of Department or County rule, policy, or reasonable expectation; illegal; or in furtherance of illegal activity. If an incident is captured on the System that has training value, such footage may be used for training purposes only when the identity of any individuals on the video is redacted and/or blurred, unless the individual has expressly authorized use of the video for training purposes without redacting/obscuring the individual’s image.

Each System shall be used in a legal manner and shall not be used in areas where there is a reasonable expectation of privacy, such as restrooms, lactation accommodation rooms, or other areas where an individual would reasonably expect not to be recorded even if there is signage on-site indicating the presence of video monitoring. Each System shall not be used for personal purposes or to harass, intimidate, or discriminate against any individual or group.

Video security cameras covered by this Policy shall not have audio, thermal, or facial recognition capabilities, nor shall they be integrated with biometric technology, without the Board of Supervisors first approving a specific Surveillance Use Policy for those cameras that accounts for those capabilities and/or integrations, as required by the County’s Surveillance-Technology and Community-Safety Ordinance.

3. Data Collection

The data collected shall be recorded video footage and may include still images obtained from that footage. Images of individuals who visit, work at, or pass by County facilities may be captured by these video security cameras since permissible video areas include, for example, County facility perimeters, entrance/exit areas, lobbies, and parking lots.

//

//

//

4. Data Access

Access to live video and recorded footage shall be restricted to the following:

- Department Head(s) and Building Manager(s) responsible for the facility and their written designee(s);
- County Executive, County Chief Operating Officer, Deputy County Executive(s) with oversight responsibility of department(s) in the facility, County Counsel, and their written designee(s);
- Director of Labor Relations and written designee(s), when evaluating a specific issue, incident, claim, complaint, case, or grievance related to the facility;
- the Director of Facilities Security and written designee(s), and security personnel specifically assigned to the facility, if any (e.g., Protective Services Office staff assigned to Santa Clara Valley Health and Hospital System (SCVHHS) facilities); and
- the Sheriff, as well as Deputy Sheriffs and other Sheriff law enforcement staff members assigned to the facility, if any.

Reasonable efforts shall be made to keep the total number of designees with access to live video and recorded footage as low as reasonably possible. Individuals not specifically authorized by this Policy to designate data access to others shall not grant data access to others. Individuals specifically authorized by this Policy to designate data access to others shall only do so in writing and only for County business purposes and subject to the limitations described in Section 2 of this Policy. For individuals specifically authorized by this Policy to grant access to others, it shall be permissible to grant access on a restricted basis, such as only allowing access to footage recorded on a particular date or only granting data access for a time-limited period.

County information technology (IT) staff members responsible for the functionality of the System shall also have access for the limited purpose of performing technical functions, such as installing or maintaining the equipment, and assisting authorized personnel in accessing data. IT staff members shall not review stored video footage without written approval from an individual authorized above to provide that written designation.

A County employee with a legitimate County business reason may request limited access to footage. Data access shall be limited to the greatest extent possible to help ensure the integrity of the data footage. To receive access, a County employee with a legitimate County business reason to access the data shall submit a written access request for a specific incident, issue, or case. That employee shall submit the written request to either the Department Head responsible for the facility, the Director of Facilities Security, or their written designee. The requesting employee shall not have access to the requested footage until the employee receives written approval from the relevant Department Head, Director of Facilities Security, or written designee; or an individual specifically identified above as having authority to designate access (e.g., County Executive, Chief Operating Officer, etc.). The Department Head and/or Director of Facilities Security, as applicable, shall consult with County Counsel prior to granting access.

To the extent access is granted, it shall be granted in writing and only for the reasonably necessary amount of footage or data necessary for the specific incident or case, and only for the amount of time required to support reviewing or investigating an incident or case as part of the employee's County job duties.

For California Public Records Act (CPRA) requests, see Section 7 of this Policy.

5. Data Protection

Video footage shall be stored in a County approved, secured location or system that is protected from intrusion by the County's network security and encryption services. Any data or footage stored on the cloud shall be through a County cloud service provider approved by the Information Security Office and shall be maintained on servers located within the United States. The system shall follow relevant Information Security Office requirements and, if network enabled, shall be segmented from the County network.

6. Data Retention

The original video footage shall be retained for the minimum amount of time necessary to meet applicable legal requirements or County, Board, or Department retention policies based on legitimate County business reasons. Once those minimum retention requirements have been met, if any, the video footage shall be deleted or recorded over. Where no other legal or retention requirements exists, then video footage shall be deleted or recorded over no later than 90 days after recording takes place.

It shall be permissible for copies of video footage to be made for training purposes. It shall be permissible for those copies to be retained for only as long as the training provides value to the Department or as long as required by applicable legal requirements or County, Board, or Department policy.

It shall also be permissible for copies of video footage to be made to fulfill the County's legal obligations (e.g., legally mandated evidence preservation or another legal obligation) and to assist with the identification, assessment, investigation, and reporting of specific behavior or specific activity that legitimately appears to be: in violation of Department or County rule, policy, or reasonable expectation; illegal; or in furtherance of illegal activity. It shall be permissible for those copies to be retained for only as long as needed to fulfill the County's legal obligation or, as applicable, for a specific assessment, investigation, or case, after which the copies shall be destroyed promptly unless they are required by law or criminal process to be retained for a longer period of time. Any data collected through video security cameras retained for specific investigative purposes shall be uploaded to an approved storage device promptly upon determining that need. Such data shall become part of an investigatory file subject to existing protocols for evidence retention.

7. Public Access

Members of the public shall not have direct access to footage captured by video security cameras. If the County receives a California Public Records Act (CPRA) request for stored

video footage, or if a subpoena or court order is issued for that footage, the data shall only be made public or be deemed exempt from public disclosure pursuant to state or federal law after consultation with the Office of the County Counsel.

8. Third-Party Data-Sharing

Sharing of data shall be limited to the following:

- District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- Public Defender's Office or other criminal defense attorneys (via the District Attorney's Office) in accordance with California discovery laws;
- Parties to litigation, in response to a subpoena or civil discovery;
- County Personnel Board and an employee's representative if the data is used as a basis for discipline, or an arbitrator or Court regarding a County administrative action or litigation;
- Other third parties, pursuant to a Court Order.

Additionally, it shall be permissible for data to be shared with law enforcement agencies and County-retained investigative personnel to assist with the identification, assessment, investigation, reporting, and prosecution of specific behavior or specific activity that legitimately appears to be: in violation of Department or County rule, policy, or reasonable expectation; illegal; or in furtherance of illegal activity.

Notwithstanding the parties identified above, no data shall be shared in a manner that contradicts Board Policy 3.54 – Cooperation with U.S. Immigration and Customs Enforcement.

9. Training

Personnel involved in accessing the System shall be trained regarding the technology as well as the need to safeguard the footage it captures; and they shall receive a copy of this Surveillance Use Policy.

10. Oversight


The Director of Facilities Security, along with any Department Head responsible for management of a facility or location with security cameras to which this Policy applies, shall oversee compliance with this Policy. Those Department Heads or their written designee shall maintain records of access to the security camera data collected and disseminated, including maintaining records of all written designations of data access pursuant to this Policy. The relevant Department Head(s) or their written designee shall audit compliance with this Policy at least annually. In addition, it shall be permissible for the Chief Operating Officer or written designee to audit compliance with this policy at their discretion.

Departments who wish to apply this Policy to their video security cameras shall seek approval from the Privacy Office, which, in consultation with the Office of County Counsel, shall

determine whether that department's video security cameras are eligible to be covered by this Policy.

Each department with video security cameras covered by this Policy shall be responsible for submitting the information required to be included in an "Annual Surveillance Report" in accordance with the provisions of Division A40 of the County Ordinance Code, the Surveillance-Technology and Community-Safety Ordinance.

Approved as to Form and Legality

 FOR SAM CRETCHER 7/5/23
Sam Cretcher
Deputy County Counsel