County of Santa Clara
Technology Services and Solutions Surveillance Use Policy

Security Cameras

To facilitate protection and safety of Technology Services and Solutions visitors, staff, surveillance technology equipment (specifically, security cameras), and the data derived from the surveillance technology equipment

1. Purpose

This Surveillance Use Policy ("Policy") shall be for the sole use of the Technology Services and Solutions ("TSS") department, located at 1555 Berger Drive, Building #2.

TSS shall maintain and operate security cameras at its public front entrance area, loading dock, and server room. The purposes of these cameras shall be to monitor and protect TSS's data center technology equipment, other assets, and electronic information. TSS may use information and images produced by the security cameras to identify and investigate potential suspicious or illegal activity, to investigate complaints by employees and customers, and to provide local law enforcement authorities with images or video clips of potential suspicious or illegal activity. Security cameras shall also be used to monitor the visitor and vendor entrance to the building and the data center outside of normal County business hours, to determine if someone is seeking entrance.

Equipment used: Axis interior surface mounted fixed camera, Axis P3225LV MKII
Axis exterior surface mounted mini dome camera, Axis P3225LVE MKII

2. Authorized and Prohibited Uses

The security cameras and the images/video they capture shall be used for County business purposes only, including the uses identified in Section 1 of this Policy, and not for personal use or other non-County uses. The use of the security cameras shall be 24 hours a day, 7 days per week, and 365 days per year within and outside of TSS's site at 1555 Berger Drive. The security cameras and their recordings shall be used in a lawful manner.

To limit any expectation of privacy, a sign shall be posted on-site at County TSS facilities to indicate the presence of video monitoring. The cameras shall not be used in areas where there is a reasonable expectation of privacy, such as restrooms, changing rooms, lactation accommodation rooms, showers, or other areas where an individual would reasonably expect not to be recorded despite signage on-site indicating the presence of video monitoring. The cameras and their recordings shall not be used to harass, intimidate, or discriminate against any individual or group.

For purposes of this Use Policy, County business shall include use for County administrative, civil, and criminal investigations and monitoring activity to protect against harm to persons or property. It shall be permissible for data collected from the cameras to be used for the following public safety and County investigation purposes:

- To assist in identifying and preventing threats to persons and property.
- To assist in identifying, apprehending, and prosecuting offenders.
- To assist in gathering evidence for administrative, civil, and criminal investigations and court actions.
- To help public safety personnel respond to emergency events.
- To assist in investigating and resolving staff and customer complaints and/or issues relating to conduct of the public or employees

TSS management shall be permitted to review images or video footage to protect TSS's technology equipment, assets, and electronic information; and to respond to law enforcement inquiries, to investigate complaints by employees and customers, and to provide local law enforcement authorities with images or video clips of potential illegal or suspicious activity.

3. Data Collection

TSS security cameras shall collect and record video images and still photography images.

4. Data Access

Access to live images and live video footage shall be restricted to:

- Chief Information Officer or designee with a County business need to access the data, in compliance with this Policy, including if the Chief Information Officer determines that access is reasonably necessary for a specific, criminal, civil, or administrative investigation or action.

- Chief Operating Officer or designee with a County business need to access the data, in compliance with this Policy, including if the Chief Operating Officer determines that access is reasonably necessary for a specific, criminal, civil, or administrative investigation or action.

To access archived images and archived video footage, approval shall be obtained from the Chief Information Officer or designee, or the Chief Operating Officer or designee, under the same business-need limitations to access live images and video footage.

5. Data Protection

TSS shall maintain data collected by TSS security cameras in a secure location where physical access is limited to authorized individuals and includes physical access protections and/or firewall protections from external intrusion.

6. Data Retention

TSS shall maintain/retain the data collected by TSS security cameras for a minimum period of one year but not longer than 18 (eighteen) months, unless required by law to be retained longer or longer retention is reasonably necessary as part of a specific criminal, civil or administrative investigation or action.

7. Public Access

Any requests for data collected by TSS surveillance technology equipment shall be submitted to the Chief Information Officer or his/her designee. TSS shall make reasonable efforts to preserve the data requested until the request has been processed. If a California Public Records Act request, subpoena, or court order is issued for the image/video data, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law. TSS personnel shall consult with the Office of the County Counsel to ensure legal compliance.

8. Third-Party Data-Sharing

The following third-party data-sharing shall be permissible:

- For safety, security, and/or investigative purposes, data (still images and video footage) may be shared with law enforcement agencies or County-retained investigators.

When data is requested by an employee or an employee representative regarding a specific claim, allegation, or action against the employee, the request shall be reviewed by the Chief Information Officer or his/her designee with the assistance of the Office of the County Counsel and the Labor Relations Department.

9. Training

TSS shall train personnel involved in monitoring TSS security cameras equipment and inform personnel of this Policy. The Chief Information Officer or his/her designee shall provide training on the use of data collected from TSS security cameras.

10. Oversight

The Enterprise Infrastructure Systems Division of TSS shall oversee the TSS security cameras to ensure compliance with the Policy, designate personnel who shall have access to the camera system, and ensure that access to the data complies with this Policy.

A log shall be maintained that records when access to image/video data is requested. This shall include the date, time, data record accessed, and staff member involved.

Any employees found to have violated this Policy shall be subject to possible discipline. Alleged violations of this Policy shall be reviewed by the CIO and/or his or her 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 9/4/18

Rob Coelho
Office of the County Counsel