CITY OF REDONDO BEACH		ADMINISTRATIVE POLICY AND PROCEDURES (APP)
Number: 10-57		**Subject:** Video Security Policy
Original Issue: 08-10-15	**Effective:** 3-16-25	**Category:** Risk Management, Safety and Information Technology
Supersedes: 08-10-20		

I. PURPOSE AND SCOPE

To set forth policy for the installation, operation, and maintenance of security cameras, monitors, and recording and storage equipment ("security systems") to ensure security and safety on city-owned property.

II. GENERAL INFORMATION

A. The City may install and maintain security cameras capable of capturing, monitoring, and recording activity. An inventory of the current camera location sis provided in Exhibit "A." This inventory shall be made viewable to the public on the City's website.

B. The purpose of the installation of cameras is to deter crime, provide visibility, and to safely secure areas with a high probability of criminal activity or frequently host large group gatherings, and to protect certain high-value assets.

C. The City may install and maintain equipment capable of recording and maintaining data captured by security cameras pursuant to the authorization requirements of this policy.

D. All recordings made by the security systems shall remain the property of the City. Employees shall have no expectation of privacy or ownership interest in the content of the recordings.

III. INSTALLATION & PLACEMENT

The installation and/or removal of cameras shall be authorized by the City Manager, or designee, in consultation with the Chief of Police and Information Technology Director. The determination to install new cameras shall be based on the following criteria:

A. Crime Activity Metrics: Cameras may be installed in areas with a documented history of criminal activity including:

1. A pattern of repeated incidents at a particular location.

Note: Regular analysis of incident reports and data should be conducted to identify trends and hotspots for criminal activity. This analysis will help determine the need for additional cameras, need for existing cameras to be removed, or the repositioning of existing cameras.

2. Response to or as a deterrent measure for particular types of crimes as designated by the Chief of Police with approval by the City Manager including reported incidents or threat of vandalism, assault, violent felony, etc.

B. Crime Prevention: Cameras may be installed in areas identified as high-risk for potential criminal activity to serve as a deterrent. Factors to consider include, but are not limited to:

1. Proximity to high-traffic areas or public spaces

2. Areas with limited natural surveillance or poor lighting

3. Locations with valuable assets or sensitive information

4. Locations where large crowds of people gather routinely

5. Vacant or abandoned properties

C. Voting Locations: Cameras may be installed in areas where election ballots are stored or processed and may only be engaged during an election cycle. These cameras shall only be used for the purpose of ensuring election integrity.

D. Review and Documentation: All decisions regarding the installation and placement of cameras must be documented, including the rationale and supporting data. Regular reviews should be conducted to assess the effectiveness of the cameras and adjust as needed. All new permanent (>90 day) security camera installations approved by the City Manager, or designee, shall be added to the City's inventory (10.57 Video Security Policy – Exhibit A) and made available for public viewing on the City's website.

E. Criminal Investigations: Nothing in this policy shall restrict the ability to install and maintain temporary (<90 day) video and audio recording devices for the purposes of criminal investigations conducted by the Redondo Beach Police Department or other law enforcement agencies.

IV. AUTHORIZATION TO OPERATE, ACCESS, AND MONITOR

A. Only authorized personnel may operate, access and monitor the security systems, and only in the manner specifically authorized. An internal list of authorized individuals shall be maintained by the Information Technology Department. Authorization may be provided as follows:

1. The City Manager, or designee, may authorize any employee of the City to operate, access, or monitor the security system, and such authorization is limited to the specific authorization given by the City Manager.

2. The Chief of Police may authorize any employee within the Police Department to operate, access, monitor and/or access recordings from the security system.

3. The Information Technology Director may authorize any employee within the Information Technology Department to incidentally access the security system for the purpose of system administration, troubleshooting or support.

B. Authorized personnel shall ensure that monitors and recordings of the security system are not visible or audible to unauthorized individuals.

V. PRIVACY

A. Restricted Areas: Security cameras must not be installed in areas where individuals have a reasonable expectation of privacy, such as private offices, restrooms, locker rooms, and other similar locations.

B. Data Protection: All video recordings must be stored securely to prevent unauthorized access, tampering, or loss. Appropriate measures must be taken to ensure the confidentiality and integrity of the recordings.

C. Review and Compliance: Regular reviews must be conducted to ensure compliance with privacy considerations and to address any concerns or issues that may arise.

D. Facial Recognition: Facial Recognition shall not be enabled unless approved by the City Council as a feature of the surveillance system, or temporarily in response to significant and/or active criminal threats for emergent public safety purposes as approved by the City Manager, Chief of Police and Information Technology Director.

E. Audio: Audio recording shall not be enabled outside of the Jail and Police Interview Rooms unless temporarily in response to significant an/or active criminal threats for emergent public safety purposes as approved by the City manager, Chief of Police and Information Technology Director or as required by law.

VI. RETENTION AND RELEASE OF RECORDINGS

A. Security System recordings shall be maintained for no longer than 60 days and in compliance with city, state and federal law.

B. Security Systems recordings may be released in compliance with a public records request, if permitted, by the California Public Records Act.

VII. EXCEPTIONS

There will be no exceptions to this policy unless approved by the City Manager.

VIII. AUTHORITY

By Authority of the City Manager

Mike Witzanksy

IX. ATTACHMENTS

A. Exhibit A – Camera Descriptions List