RANCHO MURIETA COMMUNITY SERVICES DISTRICT

Category:	Security	Policy # P2021-05
Title:	District Surveillance Cameras	

PURPOSE

District surveillance cameras provide accountability and transparency to the public and will provide a recording of an incident that may document conduct or enforcement activity or supplement a report.

The principal purpose of this policy is to provide the Rancho Murieta Community Services District's (District) Security Department with the appropriate procedures, policies, and responsibilities for the use of the District surveillance camera systems as well as the management, storage, and retrieval of audio/video material recorded by District surveillance cameras. Recorded data serves a dual purpose to the District by protecting both District personnel and citizens.

POLICY STATEMENT

The use of District surveillance camera systems provides persuasive documentary evidence of suspicious activities, criminal activity and other events in the District. District surveillance cameras are located throughout the District and are placed in locations that will offer views of sensitive and vital areas of the District. District personnel assigned to use surveillance camera and video systems will adhere to the operational objectives, policies, responsibilities, and procedures outlined in this policy to maximize the effectiveness and utility for the District surveillance camera system and the integrity of evidence and related video documentation. District employees who violate this policy will be subject to disciplinary action, up to and including termination.

OBJECTIVES

The District's Security Department uses surveillance systems to accomplish the following primary objectives:

- 1. To enhance Gate and Patrol Officer safety and accountability.
- 2. To accurately capture activities and events throughout the District.
- 3. To enhance the Gate and Patrol Officer's ability to document and review activities, incidents and other events for both internal reporting requirements and investigations.
- 4. To capture visual and audio evidence/information for use in current and future investigations and proceedings.
- 5. To insure the safeguarding of District property.
- 6. To protect Officers from accusations of misconduct or abuse from the general public.
- 7. To deter misconduct.

DISTRICT RESPONSIBILITIES

- The District may install and operate surveillance cameras as it deems appropriate
 in designated areas within the District. District personnel will use only District-owned
 surveillance camera systems, and not use personal recording devices when an
 event occurs.
- 2. The District will provide Gate Officers, Patrol Officers and Sergeants with training on the use of surveillance cameras and video systems.
- 3. The District will approve media viewing and duplication devices.

OFFICER RESPONSIBILITIES

- When necessary to help ensure the accuracy and consistency of accounts for written reports, Gate and Patrol Officers may contact the Patrol Sergeant or the Security Supervisor and request to review the recording of an incident in which he or she
 - Supervisor and request to review the recording of an incident in which he or she was involved.
- 2. Personnel will not erase, alter, reuse, modify, edit, duplicate, share, distribute, or tamper with any surveillance camera system, recording or storage device without prior written authorization from the Security Supervisor.
- 3. Gate and Patrol Officers will notify the Patrol Sergeant or Security Supervisor when the surveillance camera system has captured an apparent felony, misdemeanor, or DUI, or any event requested as evidence by a peace officer.
- 4. Gate and Patrol Officers and the Patrol Sergeant shall operate the surveillance cameras and video systems in accordance with the manufacturer's guidelines, departmental policy, and training.
- 5. Gate and Patrol Officers shall inspect the surveillance camera and video system at the beginning of each shift to ensure that the equipment is functioning according to the manufacturer's quidelines.
- 6. Gate and Patrol Officers shall immediately report any malfunction, damage, or theft of the surveillance camera system to the Patrol Sergeant or Security Supervisor so that a repair or replacement unit may be provided.
- 7. To reduce the risk of damage, original recordings shall not be viewed in any equipment other than the equipment authorized by the Security Supervisor.
- 8. Surveillance cameras and systems will remain in the area designated by the Security Supervisor.
- 9. Personnel will not make copies or use other recording devices to capture images on the display screen for personal use or distribution.

10. Streaming of surveillance camera footage to personal cellular phones or social media is not authorized. Personnel are explicitly prohibited from accessing recorded data for personal use or publication onto public and social media internet websites. Any violations of this prohibition will be grounds for sanctions, including disciplinary action.

SERGEANT RESPONSIBILITIES

- When an incident arises that requires the immediate retrieval of the recording, the Security Supervisor or his/her designee shall review and retain a copy of the recording in the District office. The Security Supervisor shall transfer the recording to the Security Supervisor's computer video storage file on the District's Security Server.
 - a. Upon downloading, the Security Supervisor or designee shall flag the entry as evidence to ensure that it will not be inadvertently deleted after the one-year retention period (per Government Code, Section 53160) for non-evidence or investigation related recordings.
- 2. The Security Supervisor or Sergeant shall conduct periodic reviews to:
 - a. Ensure the equipment is being used in accordance with policy and procedures.
 - b. Make recommendations for revision to the policy, procedures, officer training, or equipment needed.
 - c. Inspect for equipment damage, loss or misuse and to report and investigate the cause.

REVIEW OF DATA/VIDEO

- 1. Data captured by the District surveillance cameras is an official District record and shall be treated in the same manner as reports and evidence. All access to the system will be logged and subject to a compliance audit at any time. Access to the system is permitted on the right to know and need to know basis. Only employees authorized under this policy may review video according to the provisions of this policy.
- 2. An employee may review District surveillance camera files as it relates to:
 - a. Their involvement in an incident for the purpose of completing a report.
 - b. Prior to courtroom, arbitration, or deposition testimony.
 - c. For potential training purposes.
 - d. A supervisor desiring clarification regarding a concern from a citizen.
 - e. A supervisor, who is investigating a particular incident or accusation of misconduct, may review videos based on a supervisory need.
- 3. In no event shall any recording be used or shown for the purpose of ridicule or embarrassing any employee or member of the community.

MEDIA DUPLICATION

- 1. All cameras, equipment, recorded media, recorded images, and audio/video recordings are the property of the District. Accessing, copying, distributing, using or releasing video or audio files outside of the District or for non-Security Department purposes is strictly prohibited without specific written authorization from the Security Supervisor or General Manager. The exception is the release of recorded video/audio to law enforcement agencies with authorization from the Security Supervisor.
- 2. Requests to review or copy video/audio recordings made under the Public Records Act shall be made through the Security Supervisor. Each request will be evaluated and responded to on a case-by-case basis and in accordance with the requirements of the Act. If a recording is to be released, only the incident or incidents specifically requested shall be duplicated. The District reserves the right to redact the video to protect privacy interests of innocent or third parties not directly involved with the specific incident. The District reserves the right to decline a request for the following records: investigatory or security files compiled by the District for law enforcement or licensing purposes; any record where, on the facts of the particular case, the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record; records concerning confidential crime victim, sexual assault or child abuse images or recordings; and, any other record exempt from disclosure under the Public Records Act.
- 3. To prevent damage to or the alteration of the original recorded media, it shall not be moved or copied to, viewed in, or otherwise inserted into any non-District approved computer or other devices.
- 4. When possible and practical, a copy of the original recorded media stored in evidence shall be used for viewing by investigators, staff, training personnel, etc., to preserve the original media in pristine condition.
- 5. At the conclusion of any court or similar proceeding, investigation, other hearing involving District surveillance data, all copies shall be submitted back to the Security Supervisor for retention (except for any evidence retained by a court or as otherwise authorized by law).
- 6. Gate and Patrol Officers may review video footage of an incident in which he or she was involved before making a statement or being interviewed or examined about the incident.

MEDIA STORAGE, RETENTION AND DESTRUCTION

- 1. Recorded data from the surveillance camera systems shall be retained in the Security Supervisor's office for a minimum of one year (as required by Government Code section 53160).
- 2. After one year, if the data is not needed for evidence, training, a pending disciplinary matter, pending criminal case, civil lawsuit, claim or other proceeding, other investigative or law enforcement purpose or pending citizen complaint, the General Manager is authorized to destroy and erase the data within the computer system in a manner consistent with current District Policy.

3.	Recorded data from surveillance camera systems shall not be destroyed or erased without the General Manager's approval.