Riviera Community Club							
Policy and Procedure							
ВОТ	B219	Use of Video Camera System & Remote Monitoring Systems					
Department	Number	Title					
Philip L. Ronning							
Approved on		Signature	Board approval or N/A	Reviewed initial and date			

# **Policy**

- 1. This policy is a guide for the use of publicly located access cameras within the Riviera Community Club (RCC) in accordance with federal and state law. The aim is to protect the privacy expectations of employees and members while ensuring transparency and access to information to membership.
- 2. The RCC as an organization is committed to making the best effort possible to protecting public property and establishing and maintaining workplaces and public areas that are secure and safe for both employees and members. To enhance this commitment, the RCC allows the use of cameras in public areas.
- 3. The existence of this policy does not imply or guarantee that security cameras will be monitored in real time continuously or otherwise.
- 4. The RCC may, from time to time, provide measures of camera access on RCC property. However, the RCC is not a provider of security and shall have no duty to provide any security on RCC property. The obligation to provide security lies solely with each individually.
- 5. The RCC shall not be held liable for any loss or damage by reason of failure to provide adequate security or ineffectiveness of security measures undertaken.
- 6. A fixed camera used for recording areas for the purposes of enhancing public safety and security, monitoring areas, equipment or other property to discourage theft and other criminal activities, and for investigating and resolving incidents that take place on RCC public property

## **Procedure:**

- 1. **Camera Placement and Notification:** Cameras shall only be installed pursuant to the request of the RCC General Manager (GM).
- 2. The installation or removal of a camera must be coordinated with the RCC Information Technology Department.
- 3. Cameras may be installed in outdoor and indoor locations that are deemed public areas. Examples include public common areas such as parking lots, entrances, seating areas, service desks, and areas prone to theft or misconduct, or areas where money is stored or handled. Cameras will not be installed in areas where individuals have a reasonable expectation of privacy such as restrooms or private offices.

- 4. Camera placement must also take into consideration any confidential material that could be visible.
- 5. Signs shall be posted at the entrances to RCC buildings or other public facilities informing the public and staff that cameras are in use, and new employees will be notified upon hiring.
- 6. Responsibilities: The GM is responsible for overseeing the installation, maintenance, and utilization of cameras on RCC property, along with implementation of associated standards and procedures. Pursuant to this policy, the GM may delegate certain responsibilities to other RCC employees. It shall be the IT Manager's responsibility to maintain all video recordings and prepare the annual budget for the costs of maintenance, server storage, and future equipment replacements. To maintain uniformity, purchase, installation, and maintenance of camera equipment will be completed by the IT Department. Employees and members shall be notified of any new cameras installed. Cameras shall be checked weekly by the IT Department to make sure all cameras are working properly, the image quality meets the RCC's needs. Any cameras found not meeting these standards will be recommended for repair or replacement. The IT Manager shall inform the Risk Manager when a camera is found to be not working properly.
- 7. Access and Monitoring: The GM and other authorized personnel may monitor and review camera live feeds and recordings as needed and appropriate to support investigations. IT Department personnel will monitor and review security camera live feeds and recording as needed to troubleshoot and support the camera system, software, and the GM. Requests for video camera footage by an RCC member will be handled in accordance with the RCC's policy on Sharing of Information and procedure for requesting documents.

### 8. Data and Storage:

Video footage will be stored on servers accorded appropriate computer security with access by the GM and personnel authorized by the GM. Video Camera footage is the property of The RCC and will be securely retained by IT for at least 7 days and then erased, unless retained as part of a criminal or civil investigation or court proceeding, or as approved by the GM.

### 9. Location of Cameras:

There are three (3) cameras at the RCC Business office, one outside the entrance and two inside the office. There is one camera at the entrance to the Golf Pro Shop, and a total of 14 cameras at the Lake Shore Restaurant. The Lakeshore cameras are the only cameras that record audio. All current and new employees shall be notified of all camera locations as they change or increase moving forward.

#### **References:**

Washington Privacy Act: <u>RCWs</u> > <u>Title 9</u> > <u>Chapter 9.73</u> > <u>Section 9.73.030</u>

Washington State has stringent privacy laws, with <u>RCW 9.73.030</u> establishing it as a two-party consent state. This means that recording conversations without the consent of all involved parties is a criminal offense.

To be deemed private, communication requires both a subjective intention by the parties for it to be private and a reasonable expectation of privacy. Consequently, recording a private conversation in Washington is unlawful unless all parties give their approval.

To ensure the legality of recorded communications, at least one participant must announce their intention to record the conversation and include this announcement in the recording, as per RCW 9.73.030. Compliance with these regulations is essential to avoid legal repercussions and uphold privacy rights in Washington State.

However, there are exceptions:

For example, wire communications or conversations related to emergencies, threats, anonymous or inconvenient circumstances, or hostage situations may be recorded with the consent of one party.

Moreover, employers in WA State should establish policies on how long recorded footage will be retained and who will have access to it to respect individuals' privacy rights. Access to recorded footage should be limited to authorized staff and used only for lawful purposes. Transparency is crucial and adequate notification ensures that employees are aware of the monitoring activities and can make informed decisions.

Likewise, recordings must not be utilized for illegal purposes. Specifically, recordings should not be used to infringe upon employees' rights protected under the <u>National Labor Relations</u> <u>Act</u>, which bans the recording of union activities or using recording devices to intimidate union members or individuals considering union membership.

Additionally, if your workplace is unionized, it is likely necessary to engage in bargaining regarding the installation of recording devices before proceeding.