**SRR&PC Range Audio/Video Surveillance Program Description**

**2/12/2024**

**REQUIREMENTS**

1. Standard Operating Procedure (SOP) CHAPTER III. Bylaws, Article 7. Officer Duties e. IT Manager

*The IT manager shall have charge of the club computerized business systems to include hardware, software, and cyber security. Business systems include but are not limited to the club website, membership list, document archive and retrieval system, range gate access control system, range video surveillance system.*

1. Standard Operating Procedure (SOP) Appendix 2 Disciplinary Action

*In order to improve safety and enjoyment of the ranges, the Club has installed a video security**system. Recordings made by the system will be reviewed on a regular basis to verify that the range rules are being observed by all members and guests.*

*Violations of rules which could potentially or actually result in personal injury to any individual will be dealt with in a decisive manner which may result in penalties up to and including suspension of member privileges or permanent expulsion from the Club. .*

**Objective:** Provide a surveillance program to periodically monitor activities on the range to identify safety and security violations and other opportunities for improvement while supporting enforcement of the Standard Operating Procedure (SOP). The surveillance program will be limited to “public” spaces in which members should have no expectation of privacy. These spaces are specifically the parking areas, the firing line under the shelter, and the actual range from the shelter to the rear berm/backstop on each of the three ranges (i.e. Left Pistol, Right Pistol, and Rifle). All surveillance is to be performed consistent with South Carolina and Federal surveillance laws.

**IMPLEMENTATION**

* **IT Manager:** The IT Manager (or designee when the IT Manager is unavailable) has primary responsibility for design, installation and operation of hardware software, network interface and data storage services necessary to support surveillance of range activities. The IT manager reports to the EC and will request funding as necessary to keep the surveillance system up to date as new technologies become available. The technologies employed will be sufficient to add in the identification, analysis, and determination of safety and security violations. The technologies will include as a minimum live footage and recording of audio, and video data with motion detection. The technologies employed will also include remote (offsite) access capabilities.
* **CRSO:** The CRSO (or designee when the CRSO is unavailable) is responsible for periodic monitoring of surveillance system live footage and recorded clips of activities on the range. The CSRO will analyze footage and make determinations of violation. Audio/Video clips will be downloaded from the surveillance system when evidence of violation is identified to document the activities and conditions surrounding the violation. Violations including Audio/Video clips will be communicated to the individual or individuals that are involved in the violation. Violations including Audio/Video clips will be communicated to the EC, in cases which could potentially result in personal injury to any individual for proper disposition. Violations will also be included in the monthly Range Safety Report.

**SURVEILLANCE PROGRAM REPORTING**

* **Data Collection, Storage and Analysis:**
	+ Access to the surveillance system and or to data that has been stored by the system is limited to those individuals that have responsibility for the system or the data recorded from the system. The individuals that need access are:
		- IT Manager
		- CRSO
		- Technical support
	+ Live footage and recordings will be temporally stored at a secure offsite data storage service (e.g. Google Aware Plus) for a period of time sufficient to allow for the review and analysis of footage when investigation of violation becomes apparent. The data will be erased at the end of the period and will not become a record for retention.
	+ When Audio/Video clips are required to document a violation, the data will be downloaded on a club owned device (e.g. Tablet, PC…) and stored at a club contracted data storage service (e.g. Google Works) This data will not be located on a personal device or personal storage media. When technical support is required to troubleshoot the cameras or other system components, technical support personnel may use their personal devices to access the cameras and other system components, but no Audio/Video data is to be downloaded or recorded to the personal device.
* **Reporting**
	+ A surveillance system log will be developed and maintained to document the Audio/Video monitoring activities when downloads are required in a violation investigation. The log will be included in the monthly range safety report. The log will include, at a minimum:
		- Date & Time,
		- Camera(s) monitored.
		- Purpose of the monitoring
		- Comments of what was observed including any violations that were identified.
		- The file name(s) of any Audio/Video clips that were downloaded for retention.

**PROGRAM IMPROVEMENT**

* **Revise as Necessary:** Revise as necessary based on program performance, feedback and suggestions from the EC or other members.