I. PURPOSE

Security cameras are effective in reducing crime and aiding in the identification of criminals, and in identifying traffic problems and situations where the public may need assistance. The purpose of this policy is to provide guidance in the effective management of the University of Rhode Island’s (URI) closed-circuit television (CCTV) system and to establish procedures for the assessment and maintenance of surveillance/security cameras that are owned and operated by the University of Rhode Island. CCTV cameras are not monitored 24/7, however, these cameras are used as a crime prevention tool to act as a deterrent within the community.

II. POLICY

The University of Rhode Island Department of Public Safety (DPS) is committed to enhancing the safety of the University community. Toward this end, DPS will regulate the use of security cameras on the URI campuses to monitor and record public areas for reasons of safety and security and to assist in the investigation of incidents that occur on the campuses. Safety and Security purposes include, but are not limited to, protection of individuals, including students, faculty, staff and visitors; protection of University-owned and or operated property and buildings, including building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, and
cashier locations; monitoring of common areas and areas accessible to the public, including transit stops, parking lots, public streets, and pedestrian walks; investigation of criminal activity; protection against acts of terrorism or related criminal activity; and protection of critical infrastructure as defined under the USA Patriot Act or the United States Department of Homeland Security.

III. DEFINITIONS

A. Security Camera System (SCS): A system that monitors and/or records a specific location or activity for safety and security purposes on University premises, including closed circuit television cameras (CCTV) and License Plate Readers (LPR) cameras.

B. Security Camera System Owner: Department official responsible for monitoring the operation of a specific security camera system on University premises, with corresponding access rights to live and/or recorded surveillance footage from that system.

C. Avigilon Camera System: Is both a software and hardware CCTV solution. This system is capable of recording analog and digital video from IP (Network) cameras.

D. Infrared (IR) Surveillance Cameras: Cameras that have the ability to capture video in low light and no light areas. Infrared cameras are sometimes referred to as IR cameras or "Night Vision Security Cameras" because of this feature. IR Cameras can capture acceptable video in total darkness and even better-quality video in low light. Not all cameras have infrared capabilities.

E. Pan Tilt Zoom (PTZ) Cameras: Cameras that have the ability to pan, tilt and zoom, providing more system flexibility. An operator has the ability to move the camera, which allows a quick response to ongoing events.

F. Appearance Search: Video analytics technology is a sophisticated, deep-learning artificial intelligence (AI) search engine for video. It sorts through hours of video with ease to quickly locate a specific person or vehicle of interest across an entire site or multiple sites.

G. Digital Video Recorder: Sometimes referred to as a DVR. A DVR is an electronic device that records video in a digital format to a disk drive, USB flash drive, SD memory card or other local or networked mass storage device.

H. Closed Circuit TV (CCTV): CCTV refers to the use of video cameras to transmit a signal to a specific place on a limited set of monitors to view, observe, or monitor areas of interest that may include high crime areas, high security areas, or areas for surveillance data.

I. CCTV Operator: Any DPS employee authorized (Authorized User) and trained to operate the CCTV monitoring system at any given time.

IV. PROCEDURE

A. Administration of Security Camera Systems
   1. The University of Rhode Island Department of Public Safety (DPS) oversees and coordinates the installation, use, and/or removal of SCS on all URI campuses. The Director of Public Safety & Chief of Police (Chief) approves all use of SCS equipment on University property, other than as provided for in Section IV.J. Exceptions, and shall maintain a list of all approved SCS on URI campuses.
   2. A University department wishing to install a Security Camera System may select one of two options:
a. A stand-alone installation at its location, for which the requesting department will act as the SCS owner and have responsibility for management and maintenance of that system;

b. Use the University’s centralized system for which the Department of Public Safety is the SCS owner.

3. With either option, the camera feeds must be viewable in real time by the Department of Public Safety in the Public Safety Dispatch Center, Emergency Operations Center (EOC), and/or other locations as specified by the Chief.

4. All SCS equipment must be compatible with the University’s centralized system unless covered by an exception.

5. The University must comply with the terms of Sec. 889 of the John S. McCain National Defense Authorization Act, which disallows the purchase of security camera systems from certain vendors. This will be coordinated by the Department of Public Safety with input from the Division of Research and Economic Development.

6. The existence of this policy does not imply or guarantee that security camera images will be monitored in real time. The University of Rhode Island assumes no additional liability for campus safety as a result of utilizing SCS and/or making determinations of when a system is or is not monitored in real time.

B. Assessing Conditions for Camera Locations and Installations

1. Proposed locations for cameras must adhere to all applicable state and federal laws as well as any applicable University of Rhode Island policies.

2. Video monitoring/recording for safety and security purposes will be limited to locations that do not violate anyone’s reasonable expectation of privacy as defined by law. The URI Office of General Counsel will be consulted whenever there are questions about the applicability of current law or legal precedent or whenever legal advice otherwise appears to be needed.

3. Wherever feasible, cameras must be in plain view for the community to easily identify:
   a. Covert cameras may only be utilized with specific authorization for surveillance that is limited in scope, for a specific period of time, and requested by the URI Police Department or the Office of the General Counsel;
   b. Decoy, fake, or otherwise inoperable cameras are not permitted.

4. When assessing the conditions for camera locations, the following should be taken into consideration:
   a. Accessibility to power feed;
   b. Accessibility to network feed;
   c. Funding/Cost;
   d. Lighting conditions;
   e. Foliage;
   f. Field of view;
   g. Camera Capability;
   h. Operational need based upon crime prevention and crime analysis.

5. Security Camera Systems will not have the ability to record sound except where permitted by law as in the police interview room, police processing area and the cell block area.
C. CCTV Monitoring Responsibilities

1. All Dispatch Supervisors, Dispatchers, Detectives, Police Officers, Security Officers and the DPS Lead Information Technologist are considered to be CCTV system operators.

2. Dispatchers, Police Officers, and Security Officers (CCTV Operators) who are assigned to dispatch are tasked with monitoring and evaluating the positions of CCTV cameras for unauthorized movement, tampering and/or excessive foliage growth that would mask the cameras’ preset field of view, all of which should be logged and reported to the Public Safety Lead Information Technologist for modifications if needed.

3. Department members considered system operators of CCTV equipment shall utilize the system consistent with policies and procedures named in this policy and in their Job Description.

4. Operators should notify the Public Safety Lead Information Technologist of system failures and call URI Public Safety Dispatch regarding suspicious and/or criminal activity where police or security assistance is necessary for intervention.

5. Cameras are not all monitored continuously but serve as a deterrent and as an investigative tool if an incident occurs. If an incident is reported, Dispatchers should utilize the system, if possible, to provide responding police officers with up-to-date information.

6. Authorized personnel may monitor public areas for criminal activity, property and building protection, alarm verification, pedestrian or vehicle traffic activity, and any other areas where the community may need Public Safety assistance.
   a. Authorized personnel will not monitor areas where there is a reasonable expectation of privacy such as dorm rooms.

7. CCTV Operators are prohibited from using the CCTV system for purposes of monitoring individuals or areas for the following reasons:
   a. On the sole basis of characteristics of race, gender, ethnicity, sexual orientation, disability or other protected classes of people as defined in General Order 4.17;
   b. Continuously monitoring people engaged in intimate behavior in public or private areas;
   c. Viewing private areas or rooms through windows, and/or;
   d. Using the system for any purpose other than those for which it was designed and implemented.

D. Media Retention Schedule

1. Recorded events are stored temporarily on a DVR hard drive unless retained as part of an incident report, criminal investigation, court proceeding, or other legitimate use as approved by University legal counsel.

2. The DVRs must be capable of storing continuous video for up to a minimum of 30 days.

3. Unless otherwise needed, video over 90 days old will be purged.

4. Recordings will be retained in a secure location and only accessed by authorized personnel.

5. All potential Security Camera System Owners must complete a Security Camera Request Form which can be found on the DPS website.

6. Owners will maintain a list of authorized users and ensure users are removed from the system when they are no longer authorized.
7. Owners are responsible for placing approved signage to alert the public of the use of security cameras in that area. Signage must meet standards determined by the Department of Planning and Real Estate Development.

E. Security Access Protocols
1. In order to track and prevent abuse, the following protocols have been established to manage employees who are authorized to access CCTV through the DVR systems:
   a. The Public Safety Lead Information Technologist will set up the authorized client with a username and password that will be generated from their computer login access.
   b. Once the usernames and passwords are assigned, The Public Safety Lead Information Technologist will determine the following access levels of the personnel affected:
      i. Viewing video that has been recorded;
      ii. Retrieving video for investigatory purposes; and/or
      iii. Ability to move motion cameras when needed.
   c. The Public Safety Lead Information Technologist has the capability to review and retrieve video at any time.
   d. Dispatchers and Police Officers have the ability to retrieve video for up to 25 days after the event occurs. Dispatchers and Police Officers have the ability to print still shots of a requested video feed to obtain information specific to an incident or investigation.
   e. All CCTV systems maintained by the department will reside on a secure network.

F. Maintenance, Testing Responsibilities, and Video Auditing
1. The Public Safety Lead Information Technologist will log in to each Digital Video Recorder and check each camera to test for any defects. Any defects or failures will be assessed by URI Network Services to determine what actions will take place to rectify the situation.
2. Under no circumstances shall anyone except professionally trained technicians or qualified members of URI Network Services attempt to service, repair, or tamper with any of the video surveillance equipment.
3. If any CCTV system equipment fails, URI Network Services shall be notified as soon as possible. URI Network Services or a qualified vendor will be responsible for repairs and for shutting down the affected equipment during failure.
4. Auditing of CCTV videos to monitor operations is the responsibility of the Public Safety Lead Information Technologist.
   a. Auditing can be done at any time without prior notice to ensure proper use and storage of video operations is taking place.
   b. The Public Safety Lead Information Technologist will produce a monthly report to the Chief which will include maintenance performed on cameras, installations of new cameras or systems, and a list of cameras needing repair including the approximate time needed to make those repairs.

G. Training of Employees
1. The Public Safety Lead Information Technologist is responsible for training authorized employees in the operation and acceptable use of the CCTV system and its capabilities.
2. New employees with this authorization will be trained by the Public Safety Lead Information Technologist during in-service training upon hire.
3. Any person with authorization to utilize this system will read this policy and follow the guidelines of this policy.

H. Annual Reevaluation of Incidents and Camera Locations
1. An annual reevaluation of camera locations will be conducted, taking into consideration but not limited to, incident reports, feedback from police officers and detectives on the effectiveness of current cameras in their investigation of incidents, and suggestions for placement of new cameras, Crime Prevention through Environmental Design, Crime analysis and Crime Mapping. Assessments may also include but are not limited to the following:
   a. Security Assessments;
   b. Individual university department requests;
   c. New, renovated and/or upgraded buildings, parking lots, walkway areas, etc.;
   d. New shuttle stop locations;
   e. Blue light phone installations; and/or
   f. Lighting conditions, foliage, field of view, and camera capability.

I. Requests to View Recordings and Release of Information/Data
1. All video recordings on Public Safety Systems are the property of University of Rhode Island.
2. University personnel are prohibited from using or disseminating any information from the video equipment except for official purposes.
3. All information obtained and/or observations made in the use of video security equipment are considered confidential and may only be used for legitimate security, law enforcement and student safety/community welfare purposes and for compliance with federal, state and local laws as well as University policy.
4. Information obtained through video monitoring/recording can only be used for official University and law enforcement business, will only be released when authorized by the Chief or their designee, and will be released in compliance with Rhode Island General Laws, Chapter 38-2 (Access to Public Records Act) or as otherwise required by law.
5. Restricted access to certain cameras can be issued for authorized individuals in each monitored area.
6. Lawful requests (e.g. subpoenas, search warrants) for recorded video must be forwarded to the URI Office of General Counsel, which is solely responsible for reviewing and responding to all subpoenas and search warrants.
7. No security camera systems will be accessible from the public internet. All systems must be on a private subnet that is created by IT Infrastructure Services, and is isolated from the internet.
8. If remote access is required from off campus, a University VPN connection with two-factor (2FA) authentication must be used.
9. If recordings are not requested by anyone or needed for any investigatory or prosecutorial purpose, digital images shall automatically be recorded over.
a. Video recordings requested or being held as evidence or for administrative, employment, or court action shall be documented and retained consistent with policy and procedure.

b. Any video that is requested to assist other agencies must be approved by the Chief or the University Police Major.

c. Authorized users of this CCTV System are not permitted to discuss their observations and/or use these cameras outside the scope of their job functions.

10. All systems are subject to random audits for compliance with security standards and retention policies.

11. If, in the course of collecting video information for any of the purposes outlined in this policy, the University discovers student or employee activities that warrant disciplinary action, the videotaped information may generally be used in such disciplinary action if and to the extent its use is consistent with applicable law and binding legal precedent.

12. Specifics regarding License Plate Reader Systems that may differ from this policy, including but not limited to use of data, data retention, privacy and data access, may be found in the University of Rhode Island Policy on Use of License Plate Reader Technology.

J. Exceptions

1. This policy does not apply to video recording or monitoring used for University operational, academic, media, or research laboratory purposes or to the recording of public performances or interviews provided that such activity is disclosed or readily apparent to those in view of the camera.

2. This policy does not apply to video conferencing.

3. The policy does not apply to body-worn cameras operated by the URI Police Department.

4. Cameras owned and operated by individual University departments outside the centrally managed University system which were installed and in good working order prior to enactment of this policy may continue in operation until the system malfunctions or is due for upgrade or replacement.

5. Further exceptions must be approved by the Chief or their designee.

By order of: _______________________________

Stephen Baker
Director of Public Safety & Chief of Police

All Policies have an associated signed copy on file.

Attachment: Security Camera Request Form