RICE UNIVERSITY POLICY NO. 845

SECURITY CAMERA ACCEPTABLE USE POLICY

I. GENERAL POLICY

The purpose of this policy is to regulate the procurement, installation, placement and use of security cameras to monitor and record public areas for safety and security. This policy applies to the use of security cameras for monitoring and recording and therefore applies to the premises of Rice University and to all members of the Rice community, including faculty, staff, students, visitors, vendors and contractors. In general, cameras are intended to serve two main purposes for the Rice community:

Personal Safety – To capture video, in the event an individual is the subject of harm or crime, that provides information or evidence of what occurred and who is responsible, and thereby deter crimes or harmful conduct toward individuals.

Property Protection – To capture video, in the case of lost, stolen or damaged property, that provides information or evidence of what occurred and who is responsible, and thereby deter property crimes or violations.

II. DEFINITIONS

Security Cameras – a device used to transmit a signal containing images that can be viewed remotely by authorized Rice University personnel; excludes cameras worn by Rice University Police Department (RUPD) officers or in RUPD vehicles as these are governed by RUPD departmental procedures.

Security Camera Monitoring – the viewing of security camera images in real-time by authorized Rice University personnel.

Security Camera Recording – the digital, analog or other electronic storage of security camera images.

Operators – those authorized to view live or "real-time" security camera video feeds.

Security Systems Manager – the Sergeant in charge of RUPD Investigations (or such other person appointed by the Chief of Police) who is most directly responsible for maintaining Rice's security camera operation in compliance with this policy.

III. ELABORATION OF POLICY

A. RESTRICTIONS

The use of security cameras, monitoring of cameras, or recording must conform to applicable Rice University Policies, and applicable federal and state laws. Such cameras may not be used where audio recordings are prohibited. Further, security cameras shall not be used in areas where there are legitimate personal privacy concerns. Examples of such areas at Rice University generally include, but are not limited to;

- The interior of residential/dormitory rooms
- Restrooms
- Locker Rooms, shower areas, or other areas where persons change clothes

- Private Offices
- Any space used to provide physical, medical or psychological care

An exception may be made for legitimate investigations, with approval from the Office of General Counsel and consistent with state and federal law.

B. PRINCIPLES

Rice University is committed to enhancing the quality of life of the campus community by integrating the use of technology into its safety and security program. A key component is to utilize electronic security cameras and their recordings.

To maintain personal privacy in accordance with University values and applicable laws, this policy establishes procedures and regulates the use of cameras that observe public or common areas.

1. The decision of whether to deploy security cameras and the specific placement of those cameras falls under the authority of the RUPD Security Systems Manager. These decisions will be based on risk assessments, safety concerns, vulnerabilities and historical acts of criminal behavior. When developing strategies for camera installation and placement, RUPD conducts security surveys and risk analyses pertaining to individual buildings and areas within a building, broader areas and the overall university community.

2. Video cameras (and their recorded images) will not be used to monitor the conduct of faculty, staff, students, vendors, contractors or other visitors except as part of a legitimate investigation pertaining to conduct violating the law or University policy (usually resulting from a written complaint or report). While real-time viewing is not the typical use for security cameras, this policy does not prohibit (nor does it imply or promise) real-time viewing. The Security Systems Manager will seek guidance from University Human Resources, the Office of the Provost, the General Counsel or other resources as appropriate, to ensure legal and policy compliance.

3. The live or "real-time" monitoring of security cameras will be limited. RUPD will be permitted to view live video when necessary and will be conducted only by trained, authorized personnel and at all times will be consistent with this policy and applicable law. Violations of this policy or applicable law may result in disciplinary action by the University (up to and including termination of employment) or prosecution.

4. All security cameras systems predating this Policy will be required to comply with this policy within 12 months of its effective date. Unapproved or nonconforming devices and/or systems will be removed.

C. ROLES AND RESPONSIBILITIES

1. RUPD is responsible for the implementation of this policy and is authorized to oversee and coordinate the use of all University security cameras, including installation and monitoring.

2. In conjunction with other departments such as Information Technology, Facilities, Engineering & Planning, Housing & Dining and the Office of General Counsel, this policy will be reviewed

regularly and amended as needed to meet emerging needs, contemporary standards in higher education, or changes in applicable law or other University.

3. Recordings will reside on a secure Informational Technology server and are not considered to be law enforcement records until a copy is obtained by RUPD from the secured server and placed into an incident report, investigative file or other RUPD documentation.

4. The Security Systems Manager is the person in RUPD primarily responsible for departmental compliance with this policy and will review requests for release of video recordings. No release will occur without consultation with the Chief of Police and University legal counsel. The Security Systems Manager will review and determine camera locations to ensure that each fixed location camera conforms to this policy and will be responsible for compiling the master list of camera placements at Rice University. Included with the list of camera locations will be a general description of the technology deployed and the capabilities of the cameras. The location of temporary cameras that are to be used for special events or investigations will be reviewed by the Chief of Police (or the Chief's designee) to ensure compliance with this policy and must be approved before deployment.

5. If concerns arise regarding camera placement, written requests can be made to the Chief of Police to forgo the installation of a proposed camera or for the removal of an existing camera. The Chief of Police will determine the appropriateness of an installation or removal after weighing the concern of the person(s) making the request and the safety and security of the community.

6. In consultation with the General Counsel, the Chief of Police will review any complaints regarding camera locations and determine whether the policy is being followed. The Chief of Police will decide the merits of any complaint while weighing the potential benefits in community safety against any impact on privacy and other issues raised in the complaint.

7. The Chief of Police will review all requests received by the RUPD to release recordings made under this policy. No release of recordings shall occur without authorization of the Chief except as required by law or in accordance with official requests for digital recordings directly related to a criminal investigation, arrest, prosecution, subpoena or applicable law. Absent other legal requirements, the Chief of Police will approve release of recordings only for legitimate purposes, such as to protect the University and its members from harm or for purposes of legal defense. The Chief will consult with General Counsel and Office of Public Affairs prior to the release of recordings unless the time required for such consultations would jeopardize the immediate safety or security of persons or property. In such cases, the Chief or the Chief's designee will consult with General Counsel as soon as reasonably possible.

8. The Security Systems Manager will audit camera operations, including the recording storage, on a regular basis and should recommend any procedural changes needed to ensure standards and operations conform to this policy.

D. PROCEDURES

RUPD will maintain written procedures on the installation and use of security cameras. These procedures are provided as Appendix 1 of this policy, and may be updated by RUPD with approval from Office of General Counsel.

E. REQUEST FOR SECURITY CAMERAS/INSTALLATION

1. All requests to install new or additional security cameras must be made through the Security Systems Manager and must include the following:

Proposed Location
Purpose
Name and position of departmental point of contact

2. The RUPD shall review all requests to ensure compliance with the policy and to provide subject matter expertise to the department regarding camera placement, fields of view and to coordinate installation and training.

3. RUPD shall be responsible for the coordination and installation of security camera systems by working with other Rice University departments having responsibilities such as Information Technology, Facilities, Engineering & Planning, Housing & Dining, General Counsel, Human Resources and, in some cases, outside third-party vendors.

4. RUPD shall consult with the users of the facility being considered for security camera installation unless the purpose is for a confidential or criminal investigation.

5. No department shall purchase, contract, install or attempt to install security cameras or recording equipment independent of this policy.

6. Upon the effective date of this policy, all departments currently using security cameras must provide to the RUPD an inventory of security cameras, video recording equipment, and operators. Such equipment and its use must be fully compliant with this policy within 12 months.

VII. CROSS REFERENCES TO RELATED POLICIES

Policy 805, Environmental Health and Occupational Safety Program
Policy 815, Equal Opportunity/Non-Discrimination/Affirmative Action Policy

VIII. RESPONSIBLE OFFICIAL AND KEY OFFICES

Responsible Official:	Vice President for Administration
Other Key Offices:	Rice University Police Department
	Facilities Engineering & Planning
	Information Technology

Signed David W. Leebron
President

Policy History
Issued: August 9, 2017

Appendix. Additional RUPD Procedures

(Version 8.2.17)

1. Any RUPD personnel with access to view or retrieve camera recordings are subject to this policy and are required to acknowledge their understanding and compliance with this policy prior to being granted access to security camera systems and are required each year to acknowledge their understanding and compliance.
2. All information acquired from the use of security cameras (either viewed in real-time or recorded) is considered confidential. Any dissemination of observations or other information other than for official purposes is prohibited.
3. RUPD is responsible for oversight, enforcement and quality assurance of all security cameras covered by this policy and shall randomly review camera recordings to ensure compliance with this policy
4. RUPD will limit camera positions, fields of view and capabilities such as "zooming" so as to conform to policy.
5. To ensure compliance with this policy and to protect the evidentiary value of recordings, the RUPD will limit those individuals with access to retrieve or view stored recordings to authorized staff of the RUPD. Individual departments with approved security cameras in their workspaces shall be granted access to view camera feeds, but not retrieve stored recordings except through request procedures outlined in this policy. If post-incident investigation is required, departments should contact the RUPD and complete an official report.
6. In situations where application of this policy is not clear, the Security Systems Manager will maintain the status quo of the recordings at issue but seek clarification from University General Counsel and the Chief of Police.
7. No effort will be made to conceal those security cameras located in public spaces, with the exception of official, authorized cameras being used in active police investigations and approved by the Chief of Police in accordance with this policy.
8. No attempt shall be made to alter any part of camera recordings. RUPD will configure security camera recording systems to reasonably prevent operators from tampering with, duplicating, reproducing or disseminating in an unauthorized manner any recorded information.
9. Recordings will be maintained on a secure server operated by Rice's Information Technology division. In most cases, recordings will be stored for a period of no less than 30 days and no more than 60 days, depending on configuration settings in the recording device. Once the storage of an archival device reaches capacity, stored images may become overwritten and unavailable. An exception to this procedure is a recording retained as part of a criminal investigation or judicial or administrative proceeding (criminal, civil or internal), preservation of evidence or other bona fide use as approved by the Chief of Police. Images saved for such purposes may be recorded to another storage device in accordance with applicable evidentiary procedures.
10. All Operators will be trained in the technical and policy parameters of appropriate camera use.
11. Operators will receive and review a copy of this policy with the RUPD Security Systems Manager and must provide written acknowledgment that they have read and understood its content.

12. Operators will receive training in cultural/diversity awareness.

13. Operators will not alter or augment camera angles to view private or excluded areas identified within this policy, including residential spaces or windows to such spaces.

a. Operators will not monitor individuals based on general characteristics of race, gender, ethnicity, sexual orientation, disability or other protected class covered by Rice non-discrimination policies. Operators in control of cameras shall only monitor suspicious behavior or search for suspects or particular individuals, without regard to irrelevant individual characteristics.

b. Mobile or portable video equipment may be used in criminal investigations if approved by the Chief of Police. This equipment may also be used in non-criminal investigations or during events but only for a limited duration, when there is significant risk to public safety or security, and with approval of the Chief.

c. Security cameras may be viewed live or in real-time by authorized and trained operators, though such monitoring is expected to be very limited. In each case, the monitoring of cameras shall be consistent with this policy.

d. Secondary recording of live video feeds, such as through the use of a mobile phone or other video camera, is strictly prohibited.