CAMPUS SECURITY AND SURVEILLANCE POLICY

I. GENERAL POLICY

The purpose of this policy is to regulate the installation, placement and use of security cameras under Safe campus project 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 University and to all members of this community, including faculty, staff, students, visitors, vendors and contractors. In general, cameras are intended to serve two main purposes for the university's community:

Monitoring of 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.

Monitoring of 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 ---- University personnel;

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 Command and Control Center (CCC Room) who is most directly responsible for maintaining university'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 University Policies, and applicable federal/ provincial and state laws. Such cameras may not be used where audio and video recordings are prohibited. Further, security cameras shall not be used in areas where there are legitimate personal privacy concerns. Examples of such areas at 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

HEC is committed to enhancing the quality of life of the every 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. HEC's contractor will conduct a survey and will share TSR (Technical Survey Report) regarding placement of Cameras. However, the decision of whether to deploy security cameras and the specific placement of those cameras falls under the authority of university's Security Manager or designated POC (Point of Contact) of University to HEC. These decisions will be based on risk assessments, safety concerns, vulnerabilities and historical acts of criminal behavior.
2. Video cameras recordings can only be accessed by in charge of Command and Control Center neither HEC nor any other person from University is allowed to access these video cameras recordings.
3. Video cameras (and their recorded images) by 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.
4. The live or "real-time" monitoring of security cameras will be limited. University's Chief Security officer or State security agencies/ police 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.

C. ROLES AND RESPONSIBILITIES

1. University 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. Recordings will reside on a secure Informational Technology server and are not considered to be law enforcement records until a copy is obtained by authorized university's security in charge from the secured server and placed into an incident report, investigative file or other University documentation. HEC will not be responsible any loss and misuse of recordings.

3. The University's Chief Security officer is the 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 Vice chancellor/ Rector and University legal counsel. The Chief Security officer 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 University under Safe campus project. 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 Security officer to ensure compliance with this policy and must be approved before deployment.

4. If concerns arise regarding camera placement, written requests can be made to the Chief Security officer to forgo the installation of a proposed camera or for the removal of an existing camera. The Chief Security officer 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.

5. In consultation with the University's higher authority, the Chief Security officer 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.

6. The Chief Security officer will review all requests received by the university to release recordings made under this policy. No release of recordings shall occur without authorization 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 Security officer 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.

7. The in charge CCC Room 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

HEC 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 HEC

E. REQUEST FOR SECURITY CAMERAS/INSTALLATION

1. All requests to install new or additional security cameras must be made Vice Chancellor/ Rector to HEC and must include the following:

   Proposed Location Purpose

   Name and position of departmental point of contact

2. HEC 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. HEC shall be responsible for the coordination and installation of security camera systems finalized by university POC and shall monitor only Up/down status of these cameras along with accessories from HEC Central NOC by working with University's IT team and Security departments.

4. Any security cameras Purchased, contract, install or attempt to install security cameras or recording equipment other than HEC Safe campus will independent of this policy.

5. Display clear caution at locations where cameras are installed for information of the public that they are being observed.

IV. CROSS REFERENCES TO RELATED POLICIES

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

V. RESPONSIBLE OFFICIAL AND KEY OFFICES

Responsible officers	In-charge of Command and Control Center POC to HEC
Other Key Offices:	Chief Security officer Vice Chancellor Rector/ Pro-Rector

Appendix. Additional NOC Procedures

(Version 1.1)

1. Any University 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

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. University 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. HEC on request of University will limit camera positions, fields of view and capabilities such as "zooming" so as to conform to policy.

5. 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 Chief Security officer and complete an official report.

6. In situations where application of this policy is not clear, the Chief Security officer will maintain the status quo of the recordings at issue but seek clarification from University higher authorities or HEC.

7. No attempt shall be made to alter any part of camera recordings. In-charge of Command and Control Center will configure security camera recording systems to reasonably prevent operators from tampering with, duplicating, reproducing or disseminating in an unauthorized manner any recorded information.

8. Recordings will be maintained on a secure server. In most cases, recordings will be stored for a period of no less than 07 days and no more than 15 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 Security officer. Images saved for such purposes may be recorded to another storage device in accordance with applicable evidentiary procedures.

9. All Operators will be trained in the technical and policy parameters of appropriate camera use.

10. 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.

11. Operators will receive training on site after the installation of Safe campus project.

12. 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 University 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 Security officer. 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.

    e. The policy will be reviewed periodically in light of the feedback received from the universities, faculty, students, etc., and revised as may be necessary.

VI. UNDERTAKING

On behalf of University ------- it is acknowledged that the above policies, procedures, codes, and instructions have been read, understood, circulated and will be abide

Name: _____
(Vice Chancellor/ Rector/ Chief Security officer)

Date: _____

Signature/ Stamp: _____