Policy: Use of Video Security Cameras	**Policy Number:** I-7.3
Policy Owner(s): Risk Management	**Original Date:** 7/6/2017
Last Revised Date: 7/21/2017	**Approved Date:** 8/31/2017

I. **POLICY**: In order to provide a safe and secure campus environment, JCU deploys security cameras on its campus to advance legitimate public safety, operational, and security interests, including, without limitation:

- Protection of individuals, property and buildings
- Investigation of criminal activity
- Monitoring of access control systems
- Monitoring work done by third party contractors, especially when such work is done after hours
- Confirmation of security and safety alarms
- Situational awareness of campus events

II. **PURPOSE**: The purpose of this Policy is to outline guidelines for the responsible use of security cameras on John Carroll University (JCU's) campus. This Policy seeks to balance the safety and security of the University community with the privacy interests of all its members and guests. This Policy establishes limits on the use of security cameras and video recordings generated by such equipment in order to protect the reasonable privacy interests of the University community and visitors to the campus.

This Policy is not intended to address the use of video equipment for academic, media, or operational purposes. Thus, recording of public events, lectures and performances; University-sponsored "webcams"; pedagogical, research and laboratory use of video recording; video monitoring of mechanical equipment; and other filming for purposes unrelated to campus security are not covered by the procedures outlined below. Additionally, this Policy shall not apply to monitoring equipment installed in ATMs placed by sponsoring banks.

III. **SCOPE**: All employees responsible for the purchase, installation, placement, operation and/or monitoring of security cameras as well as the storage, retention and distribution of recorded images. All employees should be aware of this policy applicable to security cameras on University property.

IV. DEFINITION:

Campus Security Committee: The Campus Security Committee shall consist of the following University Officers or their designees: The Vice President of Student Affairs, The Vice President of Finance, Chief Information Officer and the University General Counsel.

V. PROCEDURES:

The use of security cameras is to be conducted at all times in a professional, ethical, and legal manner in accordance with this and other relevant University policies, as well as any applicable federal and state laws.

A. **Placement of Permanent Equipment.** Except as otherwise authorized under this Policy, permanent security cameras are to be installed only in circulation spaces, common areas, and areas dedicated to University operations as follows:

1. Cameras shall not be installed in -- nor positioned to view through the windows of or entryways to -- areas where privacy interests are paramount, such as private offices, private space dedicated to health and counselling services, residence hall rooms, locker rooms and bathrooms;
2. Locations shall be selected by the Campus Security Committee;
3. The University will maintain a listing of all camera locations and shall make such listing available to the Campus Security Committee; and/or
4. Cameras will only be installed in classrooms as a safeguard against theft or vandalism of University equipment, and only after consultation with the Provost's Office.

B. **Special Investigatory Equipment**. In response to specific safety concerns occasioned by recurring criminal behavior or other threats being monitored by John Carroll Police Department, the John Carroll University Police Chief, and/or the Director of Regulatory Affairs and Risk Management may install cameras on a temporary basis, after consultation with the Campus Security Committee, or, in the event of an emergency, the University General Counsel or their designee.

1. Cameras shall not be installed for the purpose of monitoring workplace behavior of University employees, except as part of an ongoing investigation of criminal activity by the John Carroll Police Department or other law enforcement agency, addressing a work safety issue or as part of an investigation of workplace misconduct posing a disruption or threat of harm to members of the University community.

2. Such use must be approved by the Chief Human Resources Officer and the University General Counsel or their designees.

C. **Storage, Disposition and Release of Recorded Images**. Recorded video images will be stored for a period generally not to exceed 90 days and thereafter will be erased or "overwritten," unless retained as part of an active police investigation, or subject to a valid court or agency preservation order, a University litigation hold, or needed for legitimate training purposes.

1. Recorded video images will be stored on a secure server accessible to authorized personnel only.
2. Relevant video recordings may be released by the Director of Regulatory Affairs and Risk Management, Chief of JCU Police Department or others designated by the Campus Security Committee, after consultation with the University General Counsel in any of the following circumstances:
    a. To the Office of the Dean of Students, Title IX Coordinator, or Office of Residence Life in connection with an adjudication of an reported violation of the Student Code of Conduct, Title IX violation, or residence hall behavioral expectations.
    b. To the Chief Human Resources Officer in connection with the investigation of serious workplace misconduct.
    c. To an appropriate University administrator in connection with the University's assessment of operational needs, including facilties maintenance and repair, parking management, and snow removal.
    d. To senior University administrators to assist in the assessment of and response to actual or threatened vandalism, criminal activity or other campus emergencies.
    e. In compliance with applicable law, to federal, state or municipal law enforcement agencies for purposes of investigation or prosecution of criminal activity.
    f. To third-parties for purposes related to legitimate safety concerns (e.g. to aid in locating missing persons).
    g. To parties named in subpoenas or court orders requiring production, but in conformity with requirements of any relevant laws and regulations, and after consideration of the advisability of an opposing motion to prevent or limit release.
3. Nothing in this Policy shall be deemed to restrict the use of video recordings by the University in the defense of legal actions or other proceedings brought against it.

D. **Monitoring of Cameras**. Neither the installation of security cameras nor this Policy constitutes an undertaking by the University to provide continuous live monitoring of all locations visible through such cameras.

1. At the discretion of the Campus Security Committee or their designee, cameras may be monitored in "real time" when safety, weather, or security concerns, event monitoring, ongoing investigations, system maintenance, alarms or other situations warrant such monitoring.
2. Real time monitoring, when conducted, shall comply with the following:
    a. Monitoring shall be performed by authorized personnel trained in the technical, legal and ethical parameters of appropriate camera use, and who will receive a copy of this Policy.
    b. Monitoring shall be based on suspicious behavior, not individual characteristics, including any characteristic protected by the University's Non-Discrimination Policy.
    c. Personnel who violate guidelines set out in this Policy shall be subject to disciplinary action up to and including termination and possible legal action where appropriate.

E. **Access Logs**. The retention period for camera access logs will be at least 1 year. Request for access log information will be reviewed by the Director of Regulatory Affairs and Risk Management in consultation with the Office of Legal Affairs and the Campus Security Committee.

F. **Access Privileges**. The Campus Security Committee will be responsible for controlling access permissions and adding or removing user privileges for the server system used by University security cameras. This list will be reviewed by the Campus Security Committee on an annual basis.

VI. CROSS REFERENCE:

Corrective Action Policy