STOCKTON UNIVERSITY

PROCEDURE

Video Surveillance Monitoring and Recording

Procedure Administrator: Vice President for Facilities & Operations and Chief Information Officer
Authority:
Effective Date: October 19, 2010; October 8, 2020
Index Cross-References:
Procedure File Number: 6903
Approved By: Dr. Harvey Kesselman, President

I. PURPOSE:

Stockton University is committed to enhancing the quality of life of the campus community by integrating the best practices of campus safety. A critical component of a modern campus safety plan requires the use of video surveillance technology. The Video Surveillance Monitoring and Recording Procedure shall regulate the installation, use, and retrieval of video from the surveillance cameras at the University.

II. PROCEDURE:

A. General Principles

All recording and/or monitoring of activities of individuals or groups by University surveillance cameras will be conducted in a manner consistent with University procedures and policies, state and federal laws, and will not be based on the subjects' personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristic.

The Vice President for Facilities & Operations and/or Chief Information Officer may audit the University's monitoring operations at any time without prior notice.

This Procedure does not imply or guarantee that University video surveillance cameras will be actively monitored at any time. Areas that may be monitored on a continuous basis include but are not limited to: public areas, high risk areas, and restricted access areas/locations. Further, situations that may require additional monitoring include but are not limited to: response to an alarm, special events, and specific investigations authorized by Campus Public Safety, the Vice President for Facilities & Operations, and/or the Chief Information Officer.

Video monitoring of public areas for security purposes is limited to uses that are intended to be consistent with reasonable expectations of privacy, and generally cameras will not be installed in areas where there is a reasonable expectation of privacy. Examples include, but are not limited to, the interiors of restrooms, locker rooms, residence hall rooms, private offices, and human health care treatment

areas; however, cameras may be placed in view of the ingress and egress pathways of these locations.

All access to live or recorded video from the surveillance system shall be limited to authorized personnel and as permitted by law. The University may authorize external law enforcement agencies to have limited or full access to the University's video surveillance system on a limited or ongoing engagement. The copying, duplicating and/or retransmission of this information must be authorized the Director of Campus Public Safety, Vice President for Facilities & Operations, and/or Chief Information Officer.

An employee work area may be observed for a work-related purpose, e.g., to study a University process, to observe financial transactions or cash handling, or related to an administrative investigation. Any surveillance of an employee work area must be approved in advance by the University President or Office of General Counsel.

The University may use video obtained through the video surveillance system in disciplinary proceedings against faculty, staff, or students, or in litigation involving a person(s) whose activities are shown on a recording and are relevant to the proceeding.

B. Request for Video Surveillance System

Departments, programs, or campus organizations that wish to install fixed/permanent surveillance cameras may submit a written request describing the proposed location, type of surveillance requested, and the purpose of the proposed installation to the Vice President for Facilities & Operations and/or Chief Information Officer.

University departments including, but not limited to, Facilities & Operations, Campus Public Safety, and Information Technology Services will review the request and the Director of Campus Public Safety, Vice President for Facilities & Operations, and/or Chief Information Officer will decide whether a camera(s) should be permanently installed. Cameras will be located so that personal privacy is prioritized.

C. Special Investigations and Emergency Use of Video Surveillance

In the event of an emergency or other situation appearing to pose an imminent threat to the safety and security of the University community, the University may employ video monitoring of staff, faculty or student conduct.

The Director of Campus Public Safety, Vice President for Facilities & Operations, and/or Chief Information Officer will review the request and make a decision or recommendation to the President of the University and/or his designee regarding the scope of video monitoring, type and capability of equipment to be utilized and length of monitoring. The Director of Campus Public Safety, Vice President for Facilities & Operations, and/or Chief Information Officer may consult additional sources such as the University General Counsel, County Prosecutor's Office, the New Jersey Office of the Attorney General, or other local, state or federal law enforcement for guidance.

All requests for special investigations or emergency use of video surveillance shall be approved by the Office of General Counsel or the President of the University and/or the President's designee.

D. Release of Recordings

Requests for release of video recordings shall be made in writing to the Director of Campus Public Safety, stating clearly the reason or purpose for the release.

The Director of Campus Public Safety, along with University General Counsel and the Vice President for Facilities & Operations, will review all requests received by the Police Department to release recordings obtained through video surveillance monitoring. Exempt from this process are the release of tapes, digital images and digital video not considered government records under the New Jersey Open Public Records Act such as recordings directly related to a criminal investigation.

As part of the official release of any materials, Campus Public Safety shall maintain a record of all releases on the Department's Computer Assisted Dispatch (CAD) system. The record shall identify the person receiving the record, date, time and purpose for the release.

E. Security and Retention of Video Surveillance System Recordings

All surveillance video records shall be stored in a secure University location for a period of not less than 30 days and will then be erased or written over, unless retained as part of a criminal investigation, student or employee disciplinary investigation or court proceeding (criminal or civil). Individual departments shall not store video surveillance or access control information.

Recorded media retained for criminal or civil proceedings will be treated and secured as evidence, and subject to normal chain of custody procedures.

Video storage will be stored in a secure location with access by authorized personnel only.

No attempt shall be made to alter any part of a video surveillance recording.

F. Exceptions to this Procedure

This Procedure does not apply to cameras used for academic purposes or the general use of webcams at or by the University. This procedure also does not apply to the use of video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Examples of such excluded activities include but are not limited to: video recordings of athletic events, concerts, plays, lectures, and interviews of persons. All other cameras on campus that do not record to the University's video surveillance system, such as those found in automated teller machines (ATMs) and/or University vehicles, are exempt from this Procedure.

G. Violations

Any diversion of security technologies and personnel for reasons other than the approved uses set forth in this Procedure would undermine the acceptability of these resources for critical safety goals and is therefore prohibited. Violations of this Procedure will result in disciplinary action consistent with the rules and regulations governing students and employees of the University.

Any person who tampers with or destroys a camera or access control system is subject to discipline, up to and including expulsion and termination of employment as applicable, as well as criminal prosecution.

Review History:

	Date
Procedure Administrator	12/20/2019
Divisional Executive	12/20/2019
General Counsel	08/26/2020
Cabinet	10/08/2020
President	10/08/2020