



POLICIES OF COLORADO STATE UNIVERSITY PUEBLO
UNIVERSITY POLICY

Policy Title: Video Cameras and Recording Devices on Campus	Policy ID #: 10.03.00 Category: 10. Campus Safety Policy Owner: Vice President of Operations and Chief Financial Officer 719.549.2312
<input checked="" type="checkbox"/> Draft <input type="checkbox"/> Final	Effective Date: Last Revision Date:
<input checked="" type="checkbox"/> New Policy <input type="checkbox"/> Revision of Existing Policy	Contact(s): Director of Campus Safety and Emergency Management 719.549.2373 Email: Todd.Whittemore@csupueblo.edu

POLICY PURPOSE:

Colorado State University Pueblo is committed to providing a secure environment for members of its community and to protecting personal safety and property. Video cameras and audio recording devices are important tools in this effort. Such technologies, however, may collect private or sensitive data and images, have the potential for abuse, and must be used only to meet the University's legitimate needs for security and compliance in a manner that is sensitive to interests of privacy, freedom of assembly, and freedom of expression. CSU Pueblo allows the use of these technologies through a defined process, subject to rules and procedures governing equipment installation and access to, storage, security and use of the resulting recorded data.

The purpose of this policy is to support the use of security cameras at CSU Pueblo to deter crime, assist law enforcement, and protect people and property by regulating and controlling access to video camera systems and other recording devices and the monitoring and retrieval of the data they collect, while respecting the privacy and rights of employees, students, and campus guests.

POLICY APPLIES TO (Persons affected by):

This policy governs the use of audio and video recording equipment by the University for the purpose of protecting the safety of persons and property on campus. It does not govern the use of personal devices by individuals acting in their personal capacities.

DEFINITIONS:

Electronic Surveillance System (ESS): A system consisting of electronic devices such as cameras, microphones, audio recorders, and digital storage devices, the data from which is transmitted and/or controlled remotely via a direct or network connection, and which is designed or used for the purposes of monitoring and/or recording activities on campus for Surveillance purposes.

Security Technology Committee (STC): A group comprised of the Director of Campus Safety and Emergency Management, the Safety Compliance Manager, Associate Provost, and representatives from Information Technology and Facilities Management.

Surveillance: The use of an ESS to monitor areas for safety-related reasons including, but not limited to, crime prevention and investigation, protection of persons and property, traffic conditions, accident investigations, emergency response, weather and natural conditions, crowd size, auditing cash transactions, facilities maintenance and construction, and campus events.

POLICY:

Restrictions on Electronic Surveillance Systems

Except as otherwise provided in this policy, all ESS devices and equipment shall be installed and used only for the legitimate security and business purposes of the University after review and approval by the STC.

Electronic Surveillance is normally not appropriate in areas where personal privacy is reasonably expected, such as inside a campus residence hall room, public or private bathroom, locker room, private office, or other private location. Installation of ESS devices in such areas shall not be permitted unless there are compelling circumstances (such as a criminal investigation of ongoing or threatened activities) and appropriate measures have been taken to protect privacy.

Audio and video equipment may be used as part of a fire, smoke, hazardous materials, or intrusion detection and alarm system, to monitor the condition and functioning of mechanical equipment, and the like. Such uses are not for the purposes of Surveillance and not covered by this policy.

Installation and use of audio and video equipment for educational, social, promotional, or research purposes, rather than for safety-related purposes such as those described above, is not Surveillance within the scope of this policy. For example, lectures may be recorded for educational purposes; researchers may use video cameras to document laboratory activities,

monitor climate changes, or capture and document other natural occurrences; or an event, speech, conference, or gathering may be recorded for promotional or historical purposes.

No ESS installation shall be permitted to be used for the targeting of individuals based upon perceived individual characteristics or classifications such as race, gender, ethnicity, sexual orientation, or disability.

This policy and its provisions are not intended to prohibit campus security officials, law enforcement, CSU System Department of Internal Audit, Office of the General Counsel, or their respective agents from conducting investigations and operations that may include the use of ESS devices without the prior approval of the STC.

Privacy Concerns

Surreptitious Surveillance

In general, Surveillance audio and video recording on campus may not be done in secret. Only the Director of Campus Safety and Emergency Management and law enforcement officials may authorize surreptitious monitoring and recording (with a warrant, where required). This does not necessarily mean that all areas in which ESS devices are located will have signage to this effect.

Audio Recording

In general, people have no reasonable expectation of privacy in public areas. However, people do not necessarily expect the use of audio recording anytime that video Surveillance is in use. The use of audio recording equipment has the potential to chill the free and open discourse that is inherent to the University's character, role and mission of higher education. Therefore, installation and use of audio recording equipment for Surveillance should be restricted to areas where a compelling case is shown for such measures. Such devices must be installed and used in a manner that is as non-intrusive as possible and does not unreasonably infringe upon the free and open discourse of ideas, learning, and expression of speech or of the press. The duration of the installation should be as short as possible under the circumstances. Access to recorded audio should be strictly controlled, limited and secured. Where permanent audio recording installations are approved, adequate notice of their presence should be provided, unless doing so would negate the legitimate reasons for their installation, and/or would create or perpetuate an unsafe situation.

Video Surveillance

People in public places also do not necessarily expect that video Surveillance will be capable of capturing such minute detail as the content of text messages or emails appearing on their mobile devices. Video Surveillance should be no more detailed or intrusive than is necessary to carry out its legitimate, intended purposes.

Notwithstanding the foregoing, ESS may be used to view the screens of university-owned computers in other public-access areas, and provided for public use, where personal privacy in viewing the screen is not reasonably expected.

Performance Management

ESS devices are not to be used for purposes of evaluating employee job performance, except as related to a behavioral concern, audit, safety or criminal investigation. For example, ESS may be used to monitor a cash-handling operation, but not to grade an employee on the quality of their performance in the normal course of their work.

Review and Approval of ESS Installation and Use

Except as provided herein, ESS devices may be installed or modified only with the prior review and recommendation of the STC and approval by the CSU Pueblo Vice President of Operations/Chief Financial Officer (VPO/CFO) and the CSU System Vice President for Information Technologies and Chief Information Officer (VPIT/CIO).

Special Considerations for Residential Facilities:

Unless otherwise required by a warrant or with the consent of the residents, camera views of residence halls, rooms or apartments must be of building exteriors and interior common areas that are generally accessible to all residents, and not assigned for private use.

Viewing within or through the windows of private rooms is prohibited except as part of an active criminal investigation authorized by law.

Access to Live Video or Recorded Data

Except as otherwise required by law or court order, access to view or listen to live or recorded ESS data shall be granted by the STC only for the legitimate business purposes of the appropriate University department. An individual who has been granted access to view live or recorded ESS data who abuses such privileges for personal gain, gratification, or curiosity shall have such access privileges revoked and may face disciplinary action up to and including termination or expulsion from the University.

In accordance with C.R.S. § 24-72-113, surveillance video recordings may only be accessed up to one year after their date of creation, and up to three years after creation if there has been a notice of claim filed, or an accident or other specific incident that may cause the recording to become evidence in any civil, labor, administrative, or felony criminal proceeding. The STC shall make a record of the reason for which the recording was accessed and the person who accessed the recording beyond the first anniversary after its creation. All recordings must be destroyed after the third anniversary of the date of the creation unless retention is needed for the reasons stated in this section.

RESPONSIBILITIES:

STC Responsibilities

The STC's responsibilities include:

1. To provide prior review of all proposed ESS installations and make recommendations for approval to the responsible officials.

2. To make recommendations to the VPO/CFO regarding the selection, implementation, and maintenance of a centralized electronic Surveillance monitoring system.
3. To define the protocols and procedures for storage, retrieval, and access to the video and audio data that is produced by ESS devices, including data retention periods, which may vary.
4. To assist the responsible administrators of affected units in non-emergency situations where temporary ESS installations will occur (e.g., law enforcement investigations).
5. To assist the Office of General Counsel regarding the release of ESS recordings directly related to a criminal investigation, subpoena, or legal proceeding.
6. To authorize, as appropriate, requests for permission for new, temporary, or replacement ESS installations and upgrades.
7. To periodically review all existing ESS installations and uses and make recommendations for changes as appropriate.
8. To make recommendations to the VPO/CFO and VPIT/CIO as to whether specific ESS devices and equipment should be locally controlled and accessed, centrally controlled, or both.

Responsibilities of Campus Units

1. Except as expressly provided in this policy, campus units shall not purchase, use, install or modify any ESS device without the prior, written approval of the STC.
2. Campus units that use video cameras or audio recorders that are not required for security and Surveillance purposes, but are solely for departmental purposes (for example, monitoring an approved research project), are responsible for all costs associated with those systems. These costs include purchase of the equipment, installation, maintenance, and software licensing. The STC will determine if the system can be a stand-alone system or will be required to be on a centralized University system. These devices are subject to all other provisions of this policy.
3. Each unit that has any departmental, standalone camera system in operation is responsible for ensuring that it is accessible for use only by such persons designated by the STC. Only Facilities Management is authorized to install a camera or other device that is attached to a wall or other structure.
4. Each unit is also responsible for reporting promptly to the Office of General Counsel any incident in which ESS devices or equipment have (or may have) recorded activity which appears to involve the commission of any illegal act, or an injury to persons or property; and for reporting any suspected crime in progress observed while monitoring a Surveillance system in real time, by immediately calling 911.

5. Campus units shall take reasonable measures to prevent tampering with and unauthorized access to ESS devices and equipment and shall store recorded audio/video data in a secure location accessible only to the appropriate designated individuals.
6. For all new or replacement ESS installations or upgrades, campus units shall confirm with the STC that integration with the university-wide ESS is possible and effect such integration as directed by the STC.
7. Campus units shall conduct, at least annually, audits of their authorized users and access levels in the ESS system.
8. Campus units can install monitors near building exits that display the external building camera views in live view only. This installation must be on a map that is required to be submitted with the Request for Video/Camera System form to the STC for review and approval. The map must show the location(s) of the monitors in the building as well as the locations of all cameras being installed. This map is usually supplied by Facilities Management.
9. Video or pictures from video may be used for training or other purposes if approved by the STC. Images taken in a public place where there is no expectation of privacy do not require a release. Contact the STC chair if you are uncertain of the requirements for your specific use.

Responsibilities of ESS Users

1. ESS users and operators must be trained in the responsible use of Surveillance technology, including the technical, legal, and ethical parameters of such use. The STC will be responsible for providing this training.
2. ESS users and operators shall receive a copy of this Policy and must sign that they have read, understood and will comply with its content.

FORMS:

- Request for Video or Recording System

HISTORY OF REVISIONS:

Adopted:

APPROVED:

COLORADO STATE UNIVERSITY PUEBLO

By: _____
Armando Valdez, President

Date: _____