Policy Title: Electronic Surveillance Systems

Effective Date: December 3, 2012

Policy Owner: Vice President for University Operations

Policy ID # 6-6001-003


Contact(s):
Security Technology Committee
Web: http://www.acns.colostate.edu/ITEC

Also Contact:
Environmental Health Services
Web: http://www.ehs.colostate.edu/
Email: EHS@ColoState.edu
Phone: (970 491-6745

PURPOSE OF THIS POLICY

The purpose of this policy is to protect the safety and privacy of persons and property on campus university property by regulating and controlling the use of electronic (video and audio) surveillance systems. The policy requires that all new installations and upgrades of surveillance systems at CSU be reviewed by the Security Technology Committee (STC) to assure that they meet certain requirements for placement, installation, use, data viewing and storage, secure access, and (where appropriate) centralized monitoring. These measures are necessary to help avoid incompatibility of systems, reduce exposure to liability arising from the use of such systems, and assure appropriate respect for personal privacy.

APPLICATION OF THIS POLICY

This policy applies to all University units and employees involved in the design, installation, and use of electronic video surveillance systems and equipment, and anyone who requests or obtains access to recorded data from such systems.
DEFINITIONS USED IN THIS POLICY

*Browse Access* – Individuals with approved browse access to the camera software would be able to look at all recorded/saved video for the cameras they are approved to access.

*Electronic Surveillance*: The use of any audio, video (including film camera) or combined audio/video device or equipment with the capacity to capture, record, and/or transmit sounds or images of places, things, and activities occurring in University-owned or controlled spaces for surveillance purposes.

*Electronic Surveillance System (ESS)*: A system consisting of electronic devices such as cameras, microphones, and recording systems, 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 electronic surveillance.

*ESS Data*: Digital video and audio data captured by recording devices that can be monitored, transmitted, stored, retrieved, or modified in conjunction with the use of an electronic surveillance system.

*ESS Device*: any camera, microphone, or other audio and/or video recording device that can capture and display or reproduce images and sounds, and/or store them as data; and any electronic equipment that, as part of an ESS, provides the capability to retrieve, transmit, or reproduce recorded audio and/or video data files.

*Export Access* - Individuals with approved export access to the camera software would be able to export all recorded/saved video for the cameras they are approved to access. This access is limited to CSUPD, the Student Resolution Center, the Office of Support and Safety Assessment, the office of Equal Opportunity, the Office of General Counsel, and Human Resources. Other users may request video export using a Video Export Request form that must be submitted to the STC chair for approval. Once approved, the video will be sent to the individual requesting the video along with a Video Export Receipt form that must be signed and returned to the STC chair.

*Live Access* - Individuals with approved live access to the camera software would be able to see live video for the cameras they are approved to access.

*Monitoring*: the use of cameras, microphones, display monitors, or other audio/video equipment for real-time observation of sounds and images.
**Permanent Installation:** The installation of any ESS device or system that is intended to remain in place for an indefinite time, and to be removed or modified only for change of circumstances, upon approval of the STC.

**Security Technology Committee (STC):** a committee appointed by the Vice President for Information Technology (VPIT) and Vice President for University Operations (VPUO) to review electronic security measures and make recommendations to the Vice Presidents regarding changes, upgrades, and issues concerning the systems, devices and procedures related to such measures. The STC Chair is appointed by and reports to the Chief of Police. Co chairs shall be the Chief of CSUPD or their delegate, the Director of Environmental Health Services, or their delegate, and one member (the ‘Members’) each appointed by the Director of ACNS, the Director of Facilities, the Vice President for Student Affairs, the Director of Risk Management and Insurance, CITAC, the Director of Parking Services and the President of ASCSU. Each member will select a backup member to attend in their absence. The Members of the Committee shall be appointed for a term of two years, except for the Member appointed by the President of ASCSU, who shall serve for a term of one year. Members may be reappointed without limitation, and such reappointments are to occur automatically unless another Member is appointed by the appointing authority.

**Surveillance Equipment Operator:** Any person viewing or controlling an ESS device or ESS system equipment.

**Surveillance:** the use of any ESS device to observe any place or thing and to capture, record and/or document occurrences or conditions, for the purpose of securing and protecting the University, its property, and persons in or around University property.

**Temporary Installation:** The installation of any ESS device or system that is intended to remain in place for a defined period, or for only as long as required for a specific investigation, trial period, or other short-term need, and is to be removed when the specified need or period has elapsed:

**Unit or Campus Unit:** A college, department, program, office, research center, business service center, or other operating unit of Colorado State University, including, but not limited to, units located on the main Fort Collins campus, any satellite campus, and any research or agricultural extension, cooperative extension, or other outlying unit location.

---

**POLICY STATEMENT**

**POLICIES OF COLORADO STATE UNIVERSITY**

Electronic Surveillance Systems
Colorado State University is committed to providing a secure environment for members of its community and to protecting personal safety and property. Electronic surveillance systems are an important tool in this effort. Such technologies, however, 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 allows the use of approved electronic surveillance systems through a defined process, subject to rules and procedures governing equipment installation and access to, storage, security and use of the resulting recorded data

**POLICY PROVISIONS**

1. 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. The following restrictions and requirements apply to all ESS installations:
   
a. The use of ESS devices and equipment shall be restricted to places where risks to the security or well-being of persons or property are legitimately of concern, or where business activities such as cash handling are subject to audit.

   b. 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 any other private location. Installation of ESS devices in such areas shall not be permitted or approved unless there are compelling circumstances (such as a criminal investigation of ongoing or threatened activities) and appropriate measures have been taken to protect privacy.

   c. ESS devices 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 also not normally expected in places where the persons being observed have a reasonable expectation of privacy.

   d. Installation and use of audio and video equipment for educational, social, promotional, or research purposes, rather than for the protection of persons and property, prevention of crime, or auditing of business activities, is not “surveillance” within the scope of this policy. For example, lectures may be recorded for educational purposes; researchers may use video cameras and
recording equipment to document animal 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. While these installations may be reviewed by the STC to assure that they are not for the purposes of surveillance, such uses are otherwise not subject to this policy (although other University policies may apply). Anyone proposing a camera to be installed on the University system is required to follow the policy procedures, complete the required forms and be approved by the STC.

e. 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. In addition, surveillance equipment operators must not knowingly, continuously monitor people engaged in intimacy in public areas unless another, legitimate reason for such observation is being served.

f. Notwithstanding the above restrictions and limitations, this policy and its provisions are not intended to prohibit the Department of Internal Audit, Office of the General Counsel, or the CSU Police Department, directly or through an agent, from conducting investigations that may include the use of surveillance systems, without the prior approval of the STC.

2. In general, people have no reasonable expectation of privacy in public areas. However, people do not necessarily expect the use of audio surveillance 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 in order to protect the campus community against an appreciable threat of harm. Such devices must be installed and used in the manner that is as non-intrusive as possible, is least likely to record academic or research activities, 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 the 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.

3. People in public places 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.

4. 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, and signage to this effect is in place.

5. ESS surveillance is not to be used as an employee performance management tool. It is not appropriate to use ESS devices to measure an employee’s performance, although ESS Data may be relevant to a determination whether any person has violated University policy or applicable law.

6. Special Considerations for Residential Facilities:
   a. 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.
   b. Viewing within or through the windows of private rooms is prohibited except as part of an active criminal investigation authorized by law.

**STC Responsibilities**

The STC’s responsibilities include:

1. To provide prior review of all proposed ESS installations;

2. To make recommendations to the AVP of Safety and Risk Services, Vice President for University Operations VPIT and the VPUO-Vice President for Information Technologies regarding the selection, implementation, and maintenance of the 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;
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 Chief of Police and 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 make recommendations to the Chief of Police as to whether specific ESS devices and equipment should be locally controlled and accessed, remotely controlled and accessed by connection to the University's central surveillance system, or both.

Responsibilities of Campus Units

1. Except as expressly provided in this policy, campus units shall not install or modify any ESS device without the prior, written approval of the STC.

2. Campus units that install cameras that are not required for CSU security and surveillance purposes, but are solely for departmental purposes (for example, monitoring a research project or gauging how many customers are waiting to be served), are responsible for all costs associated with those systems. These costs include purchase of the equipment, installation, equipment maintenance, and software licensing. The STC will determine if the system can be a stand-alone system or will be required to be on the University system. These devices are subject to all other provisions of this policy.

3. Each unit that has any ESS device in operation is responsible for assuring that the ESS device(s) and equipment are accessible for use only by such persons designated by the STC, and are adequately secured, monitored, and maintained in good working order.

4. Each unit is also responsible for reporting promptly to the STC or the Chief of Police 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 surveillance data in a secure location, accessible only to 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 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.

7.9. 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.

Storage, Retention and Access to Recorded Data:

1. All data storage will be by digital means. Stored data will be retained for a minimum of 14 days, or such longer period as may be determined by the STC. Specific applications, such as Payment Card Industry Data Security Standard (PCI DSS) compliance, may have greater retention requirements.

2. Access to stored data shall be strictly limited to University employees who have a legitimate business need. Campus units shall identify the persons within the unit who have a recurring, legitimate business need to access real-time or stored ESS data and shall provide names and positions to the STC. Persons not identified for such purposes shall not be permitted access without the express, prior, written approval of the STC Chair. **All police personnel with access to the camera system will be required to have routine background checks related to their position and will therefore have STC pre-approval for live/browse/export capabilities.**

3. The STC **may** require background checks before approving any person’s access to ESS data. **Background checks will be performed every 3 years for individuals with**
the ability to export data. Others with live or live/browse access will have background checks every 5 years. All police personnel with access to the camera system are required to have routine background checks related to their positions and are therefore not required to have 3 or 5 year background checks performed by the STC.

4. STC members must undergo background checks (as prescribed by the VP of AVP for Safety and Risk Services and the Executive Director of Human Resources) prior to serving on the STC (or, where appropriate, as soon as practicable after being appointed). In addition, all STC members must undergo training in the same manner as provided herein for Surveillance Equipment Operators.

5. Release of Recorded ESS Data:

   a. Requests for external release of recorded data must be approved by the STC Chair, who will consult with the Office of the General Counsel to determine whether such release is appropriate. Open records request? Only OGC can release?

   b. All such data released shall be specifically requested using the Video Export Request document. The person(s) to whom the data is provided shall be required to sign a Video Export Receipt form acknowledging receipt of access to, or copies of, the data, together with an acknowledgement of any limitations or restrictions on the release and any re-release.

   c. Each campus unit, whether or not it actually has ESS devices, that receives a request, demand, subpoena, court order, or any other type of request for the disclosure, release or use of ESS data shall immediately contact the STC Chair and shall secure, maintain and preserve in a secure location any data that is in the unit’s possession or control, pending the outcome of the matter.

   d. Where such requests take the form of subpoenas or other legal documents compelling production, the responsibility for responding to requests rests with the Office of the General Counsel.

Security Technology Committee (STC) Procedures, Forms, and Training:

1. The STC will meet at least quarterly, or as otherwise necessary as determined by the Chair(s), to review ESS installations, make determinations as authorized by this Policy, review requests from campus units for installation or modification of ESS
devices or equipment, review security measures, manage budget, manage software and maintenance contracts, approve server acquisitions, etc.

2. The STC will submit an annual report of its activities and determinations to the VPUO and the VPIT AVP of Safety and Risk Services and the VPUOIT.

3. The STC will make recommendations for system changes and policy changes as necessary.

4. The STC will develop procedures and forms as required for the implementation of, and compliance with this policy. Procedures and forms shall be reviewed by the Office of Policy and Compliance University Policy Office, Office of the General Counsel and the Vice President for University Operations before being adopted.

5. Opportunities for campus education and training on this Policy and STC procedures will be provided annually.

5.6. Once a request is submitted and before access is granted, on-line training and a background check must be completed and reviewed and approved by the Colorado State University Police Department. An email will be sent to the individual requesting access with a link to take the training. An email will be sent once access is granted.

Installation of ESS Devices:

Except as provided herein, ESS devices may be installed or modified only with the prior review and recommendation of the STC.

Existing installations:

Existing installations of ESS devices and systems may be reviewed by the STC to assure that they are being appropriately utilized and to determine whether the local, campus unit control and access is secure and appropriate. Any changes in equipment, security, access and control that may be recommended by the STC shall be discussed first with the unit director and, as appropriate, with the VPUO and/or VPIT Assistant Vice President of Safety and Risk Services and the Vice President for University Operations. In the event that the STC determines that a unit having one or more local ESS devices in use should be required to either grant access to CSUPD or to transmit the ESS data to the University’s central ESS system, the STC shall document the reasons for such determination and work closely with the unit to implement changes. It is the responsibility of every unit that has a local installation of ESS devices in place to inform the STC of the existence of such devices and
systems, and to not install any new devices or implement any upgrades or modifications of the equipment, without prior review and approval.

**New installations and modification of existing installations:**

New installations and modifications of existing installations must utilize equipment that is compatible with the University’s centralized ESS, unless the [VPUO and/or VPIT Assistant Vice President of Safety and Risk Services and the Vice President for University Operations](DRAFT) determines otherwise after STC review.

Campus units shall not purchase ESS devices or equipment without the involvement of the CSU Purchasing Department.

**Temporary Installations:**

A temporary installation of an ESS device or system may be authorized by the Chief of Police or the Vice President for University Operations, for purposes of aiding in an investigation, without the prior approval of the STC. The period for which the installation remains in place shall be limited to the duration of the investigation or sixty days, whichever is shorter, unless the authorizing administrator approves a longer period.

**Security concerns related to protecting the integrity of the infrastructure:**

Security of ESS equipment shall be provided in all installations, including physical protection of the cameras, DVRs, and cabling systems, as well as access to the applications and the stored video content.

Physical security of the surveillance system infrastructure must include (at a minimum) camera installation in tamper proof enclosures, installing cabling in (EMT) conduit, and locating DVR’s or servers in locked rooms with carefully controlled access.

**Surveillance Equipment Operators:**

Surveillance equipment operators must be trained and supervised in the responsible use of surveillance technology, including the technical, legal, and ethical parameters of such use. The STC will be responsible for providing or arranging for this training.

Operators shall receive a copy of this Policy and the STC Procedures standards, and must sign that they have read, understood and will comply with their content.

---

**COMPLIANCE WITH THIS POLICY**
Violations of this policy can lead to disciplinary action, up to and including termination of employment or discipline pursuant to the Student Conduct Code. Persons violating this policy may be subject to civil and criminal liability under applicable laws. If a system is installed without complying with the policy, it may be removed at the expense of the department responsible for the unauthorized installation.

REFERENCES

American Library Association, ALA Library Bill of Rights
http://www.ala.org/ala/issuesadvocacy/intfreedom/librarybill/index.cfm

Student Conduct Code

FORMS AND TOOLS

Video System Request Form Request for Video/Camera System (CSU Police Department Facilities Management website)

APPROVALS

Approved by Anthony Frank, December 3, 2012

Revision approved by Lynn Johnson, Vice President for University Operations, November 10, 2017

Revision approved by Lynn Johnson, Vice President for University Operations on