Administrative Procedure: Security Camera Placement and Acceptable Use Procedure

Purpose

Grossmont-Cuyamaca Community College District is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. A critical component of a comprehensive security plan is the utilization of a security and safety camera system. The surveillance and video recording of public areas is intended to deter crime and assist in protecting the safety and property of the campus community. This policy addresses the college's safety and security needs while respecting and preserving individual privacy and providing transparency, in the use of video camera technology in achieving a safe and secure campus environment.

To ensure the protection of individual privacy rights in accordance with the college's core values and state and federal laws, this policy is adopted to formalize procedures for the installation of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records. The purpose of this policy is to regulate the use of camera systems used to observe and record public areas for the purposes of safety and security. The existence of this policy does not imply or infer that cameras will be monitored in real time 24 hours a day, seven days a week.

Security cameras will be used in an ethical and professional manner in accordance with existing College policies, including Non-Discrimination Policy, the Sexual Harassment Policy, Family Educational Rights & Privacy Act (FERPA), local, state and federal laws and regulations and other relevant policies. This policy applies to all personnel and property of the College in the use of security camera monitoring and recording. Images and related data collected by security cameras are the property of the District will be retained for a reasonable period of time, and will be destroyed by coping over the data thereafter.

Policy

The District's Public Safety Department, in conjunction with contracted law enforcement agencies, have the authority to select, coordinate, operate, manage, and monitor all campus security surveillance systems pursuant to this policy.

This policy is to regulate the use of video surveillance and recording on District premises. All existing uses of security camera systems will be required to comply with the policy. Unapproved or nonconforming devices will be removed.

Appropriate signs and notice of video surveillance will be posted at all entrances and in random areas which are subject to video monitoring.

Employees who may require access to information collected through video surveillance will be provided proper training and orientation with regards to this Policy and their obligations under this Policy and will provide written acknowledgment that they have read and understood the contents of this policy and procedure. Any employee who knowingly or deliberately breaches this policy will be subject to discipline up to and including termination. The recording medium must be handled in a manner that maintains the integrity and security of the recorded information.

Procedure

The Public Safety Department will insure that selected Public Safety employees have access to video monitoring or recording locations, are trained in the responsible operation of video surveillance systems, have read and understand this policy and understand their legal obligations under FERPA.

1. Video recordings contain personal information and should not be viewed by unauthorized persons. Employees are not to view video information for personal interest and are under no circumstances to copy or transmit video information to anyone else except as provided for explicitly in this policy.

2. Ensure other District employees who may be required to view video information to perform their duties have read and understand this policy and their legal obligations under FERPA. All persons authorized to access video information are to sign confidentiality agreements.

3. Ensure the video monitoring password and/or access code is changed whenever the employment of someone with access to the system is terminated or is no longer is in a position that requires them to monitor video information.

4. Inform the Public Safety Department and the Human Resources Department, of any employees or service providers who do not comply with this policy. Also inform the Chancellors and Presidents Offices if a privacy breach has occurred, or may have occurred.

5. Ensure reception equipment is placed in accordance with the policy provisions regarding privacy and only in areas where they are necessary for safety or security reasons and are suitable for the conditions (exterior, interior, low light, PTZ etc.)

6. If reception equipment is adjustable by operators, this practice will be restricted, wherever possible, so that operators cannot adjust or manipulate the cameras to view spaces that are not intended to be covered by the video surveillance program.

7. Under no circumstances will cameras be directed through any District or non-District locations where persons have a reasonable expectation of privacy.

8. Ensure that no attempt will be made to alter any part of a recording.

9. Ensure that old storage devices are wiped clean and rendered unserviceable before disposal. A written record describing the date, method and location of the disposal will be retained for seven years.

10. Where a review of recorded information indicates that unlawful activity has occurred or is suspected, law enforcement will be brought in to view that recorded information. Video evidence will be stored securely until law enforcement responds. When a recording is seized as evidence, the name of the investigating officer and date and time of seizure will be recorded and retained in a log book, which will be retained for seven years.

The Public Safety Department will ensure the video surveillance data storage system and monitoring program is maintained in good working order and that all storage devices (such as DVDs, hard drives, or servers) that are not in active use will be stored securely in a locked cabinet in a controlled-access area.

The Public Safety Director will assess requests for reception equipment in accordance with the following criteria:

1. Other measures to protect public safety, detect or deter, or assist in the investigation of criminal activity have been considered and rejected as unworkable.

2. The use of each video surveillance camera should be justified on evidence based criminal or safety concerns.

3. Assess the privacy implications to minimize intrusiveness.

4. Consultation with stakeholders such as local law enforcement has occurred.

5. Applicable laws (external requests).

6. Need to know to perform authorized District functions.

7. The provisions of this policy Ensure compliance with this policy.

All recorded information shall be destroyed after thirty (30) days, excepting information specifically awaiting review by law enforcement agencies, information seized as evidence, or information that has been duplicated for use under civil or criminal subpoena. The destruction of the recorded information shall occur by overwriting the data as new video is recorded.

Camera equipment placement locations and operation shall be limited to visual access of areas where there is no reasonable expectation of privacy. Video surveillance for the purpose of monitoring work areas, staff areas, or sensitive areas will only occur in special circumstances, and must be consistent with the policy's principle purpose, which include the prevention/deterrence of illegal activity and the enhancement of safety with the prior written approval of the Human Resources Department.

When video surveillance footage is being displayed by authorized employees on a video monitor, the monitors will be in a position that cannot be viewed by others.

Responsibilities and Authority

Responsibility for oversight of security cameras and associated policies, standards, and procedures, is delegated to the Public Safety Department.

The Public Safety Department will be responsible for the creation, maintenance, and review of a campus strategy for the procurement, deployment, and use of security cameras, including this and related policies. This includes:

1. Designation of the standard campus security camera system or service and authorizing the placement of all security cameras.
2. Requesting the purchase of any new security camera systems.
3. Reviewing existing security camera systems and installations and describing required changes to bring them into compliance.
4. Creating and approving campus standards for security cameras and the procedures for the use of security cameras.

Public Safety will monitor developments in the law and in security industry practices and technology to ensure that camera surveillance is consistent with the best practices and complies with all federal and state laws.

The Public Safety Director and Vice Chancellor of Human Resources will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed.

Copies of video information obtained by security camera recording will be released internally or to law enforcement personnel only as authorized by the Public Safety Director. Copies will not be released to any other party except pursuant to valid subpoena that has been first reviewed by the college's Legal Counsel prior to the release of any records.

Security Camera Placement

1. Grossmont-Cuyamaca Community College District may establish temporary or permanent placement of security cameras in public areas of the college campus.
2. Audio recordings must have proper signage posted.
3. Security cameras will not be used in private areas of the campus unless prior written approval is obtained from the President or Human Resources and the purpose is to assist in the furtherance of a criminal investigation.
4. Monitoring private areas includes bathrooms, shower areas, locker/changing rooms, or other areas where people may change clothes, and private offices, except as noted above, is prohibited.
5. Grossmont-Cuyamaca Community College District will monitor and review security camera feeds and recordings to support investigations, or enhance public safety for the campus community.
6. Monitoring any individual based on race, gender, ethnicity, sexual orientation, disability, or other protected classification is strictly prohibited.

Use of Recordings

1. Recordings on the security camera equipment are to be used for the purposes described in the above definition of a security camera. This use extends to their release to law enforcement agencies. Records of the access to these systems shall be maintained.
2. The use of security camera footage other than which is detailed in this policy is strictly prohibited, and is subject to disciplinary action.
3. Recordings from cameras whose primary function is not security, such as the recordings from classroom lectures, may be used for the purposes described by the definition of a security camera if the situation warrants an investigation.

Retention of Recordings

Security camera footage shall be retained for a period of no less than 15 days. The retention period may be extended at the request of College legal counsel, local law enforcement, or as required by law.

Placement of Cameras

The locations where cameras are installed may be restricted access sites such as a departmental computer lab; however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located so that personal privacy is maximized.

Camera positions and views shall be limited based on the need of the camera placement. The view of a camera must not violate the standard of a reasonable expectation of privacy.

Unless the camera is being used for criminal investigations, monitoring by security cameras in the following locations is prohibited:

1. Bathrooms
2. Locker rooms
3. Offices
4. Classrooms not used as a lab

Unless being used for criminal investigations, all video camera installations should be visible.

Requests for new Installation of camera surveillance

Individual departments, programs, or campus organizations requesting video surveillance cameras shall submit a written request to their appropriate Vice President describing the proposed location of surveillance devices, justifying the need for the proposed installation, and identifying the funding source or sources for purchase and ongoing maintenance of the project.

- The Vice President or his/her designee will review the request and if approved recommend it to the Public Safety Department.
- The Public Safety Department, will review all proposals. Upon completion of review of the project, the Campus Safety and Parking Control Department will determine if the request meets the requirements of this policy or not and if it should be approved or denied.
- The President will be responsible for reviewing and approving or denying all denied proposals for security camera equipment, which have been denied by Public Safety.

The Information Systems Department (IS) shall be consulted prior to the installation of all approved security camera systems.

The Purchasing Department will not accept, approve, or process any order for security camera systems without the approval of the Public Safety Office.

Scope

This policy applies to all personnel and departments of the Grossmont-Cuyamaca Community College District in the use of security cameras and their video monitoring and recording systems. Security cameras may be installed in situations and places where the security and safety of either property or persons would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, the cameras may be placed campus-wide, inside and outside buildings. Although the physical cameras may be identical, the functions of these cameras fall into three main categories:

1. Property Protection: Where the main intent is to capture video and store it on a remote device so that if property is reported stolen or damaged, the video may show the perpetrator. Examples: an unstaffed computer lab, an unstaffed science lab, or a parking lot.

2. Personal Safety: Where the main intent is to capture video and store it on a remote device so that if a person is assaulted, the video may show the perpetrator. Examples: a public walkway, spaces, or a parking lot.

3. Extended Responsibility: Where the main intent is to have the live video stream in one area monitored by a staff member in close proximity.

This policy only applies to video surveillance activities necessary to enhance the security and safety of people and property on District premises.

Training

Camera control operators shall be trained in the technical, legal, and ethical parameters of appropriate camera use.

Camera control operators shall receive a copy of this policy and provide written acknowledgement that they have read and understood its contents.

Operation

1. Video surveillance will be conducted in a manner consistent with all existing District policies.
2. Camera control operators shall monitor based on suspicious behavior, not individual characteristics.
3. Camera control operators shall not view private rooms or areas through windows.
4. All operators and supervisors involved in video surveillance will perform their duties in accordance with this policy.

Storage and Retention of Recordings

Copies which are made of specific segments of recorded information for purposes of an official criminal investigation will be dated and labeled with the law enforcement's assigned occurrence number. Access to these copies will be limited to authorized personnel. Logs will be kept of all instances of access to, use, or release of these stored copies, to provide for a proper audit trail.

No attempt shall be made to alter any part of any surveillance recording other than selecting specific incidents or periods of time to be retained.

All video surveillance data shall be stored in a secure for a period of 30 days and will then promptly be erased by being written over by newer recorded data, unless retained as part of a criminal investigation, court proceedings (criminal or civil), or other bona fide use as approved by the Public Safety Department.

Compliance

The Director of Public Safety will ensure that records related to the use of security cameras and recordings from security cameras are sufficient to validate compliance with this policy.

1. Security camera systems procured by Departments will need to ensure compatibility with the system identified as the campus standard by this policy and the Public Safety Department.
2. All appropriate measures must be taken to protect an individual's right to privacy and hold District information securely through its creation, storage, transmission, use, and deletion.
3. All camera installations are subject to federal and state laws.
4. This policy will be reviewed by the Public Safety Department on an annual basis.
5. Any exception to the uses listed above shall be governed by applicable District policy and laws.

Appropriate Use and Confidentiality

Personnel are prohibited from using or disseminating information acquired from District security cameras, except for official purposes. All information and/or observations made in the use of security cameras are considered confidential and can only be used for official District and law enforcement purposes. Trained personnel are expected to know and follow this District Policy.

Use of Cameras for Criminal Investigations

The use of mobile or hidden video equipment may be used in criminal investigations by the District. Covert video equipment may also be used for non-criminal investigations of specific instances which may be a significant risk to public safety, security and property as authorized by the Campus Safety and Parking Control Department.

Definitions

As used within this policy, the following terms are defined as follows:

1. Security camera: a camera used for monitoring and recording public areas. A critical component of a comprehensive security plan is the utilization of a security camera. The surveillance and video recording of public areas is intended to deter crime and assist in protecting the safety and property of the campus community. This policy addresses the college's safety and security needs while respecting and preserving individual privacy, while providing transparency, in the use of video camera technology in achieving a safe and secure campus environment.
2. Security camera monitoring: the real-time review or watching of security camera video feeds.
3. Security camera recording: a digital recording of the video feed from a security camera.
4. Security camera systems: any electronic service, software, or hardware directly supporting or deploying a security camera.
5. Reception equipment: any device capable of capturing and/or recording images, including audio and thermal imaging devices.
6. Video Surveillance System: refers to a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of specific locations on District property and the actions of individuals in those locations.
7. Personal Information: is recorded information about an identifiable individual which includes, but is not limited to, the individual's race, color, national or ethnic origin, sex and age or vehicle identification information.

Exceptions

This policy does not apply to cameras used for academic purposes. Cameras that are used for research would be governed by other policies involving human subjects and are, therefore, excluded from this policy.

This policy does not address the use of Webcams for general use by the District (e.g., on the official District website). This policy 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 would include videotaping of athletic events for post-game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are exempt from this policy.

AUTHORIZED USER AGREEMENT FOR DISTRICTWIDE VIDEO SURVELLIANCE SYSTEM

All recording or monitoring of activities of individuals or groups by District cameras will be conducted in a manner consistent with District procedure, 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 characteristics. Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner. All personnel with access to District security cameras should be trained in the effective, legal, and ethical use of monitoring equipment.

District security cameras are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: high risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the Director of Campus Safety and Parking Control or his designee.

For Property Protection and Personal Safety cameras, access to live video or recorded video from cameras shall be limited to authorized personnel or other persons authorized by the Public Safety Department. The copying, duplicating and/or retransmission of live or recorded video will be limited to persons authorized by the Public Safety Department or the Human Resources Department.

A record log will be kept of all instances of access to, and use of, recorded material. Nothing in this section is intended to limit the authority of the District's law enforcement activities.

I agree to the terms stated above and agree to follow the Districtwide procedure as written.

Date: _____

Printed Name: _____

Signature of User: _____

Director of Public Safety Signature: _____