SECURITY CAMERA OPERATING POLICY

The Contra Costa Community College District (CCCCD) and its colleges are committed to enhancing the quality of life of the 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. In order to enhance security, deter crime, and protect property and the safety of members of the campus community and public, it has been determined that the use of video monitoring, video recording, or other visual digital recording equipment may prevent losses and aid in the law enforcement activities of the District Police Department.

SECURITY CAMERA OPERATING PROCEDURE

The District and its colleges are committed to enhancing the quality of life of the 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 monitoring of public areas is intended to deter crime and assist in protecting the safety and property. In order to enhance security and protect the safety of members of the public and community it has been determined that the use of video monitoring, video recording, or other visual digital recording equipment may prevent losses and aid in the law enforcement activities of the Police Department. This procedure addresses safety and security needs while respecting and preserving individual privacy.

1.1 PURPOSE

A. The District Police Department is authorized to use still cameras or video equipment to record events where there are likely to be violations of District rules, regulations, policies, or violations of law. Cameras may be operated either overtly or covertly depending on the circumstances. In the case of demonstrations, protests, and similar situations, use of cameras will be generally overt, partly as a means of deterring illegal acts. Cameras may be permanently mounted or operated from either remote locations or by automated devices. An exception to this recommendation would be if announcing the use of video monitoring would undermine its purpose.

B. To ensure the protection of individual privacy rights in accordance with the District's core values and state and federal laws, this procedure is adopted to formalize processes related to the installation of security equipment and the handling, viewing, retention, dissemination, and destruction of security records. The purpose of this procedure is to regulate the use of camera systems used to observe and record public areas for the purposes of safety and security.

C. The existence of this procedure or video security equipment does not imply or guarantee that cameras will be monitored in real time at any time.

D. All public space electronic video security equipment used will be in accordance with state, local, and federal law. Under no circumstances shall the contents of any video media be exploited for purposes of profit or commercial publication, nor shall recordings be distributed to third parties except as may be required by law. Information must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure. 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.

E. The primary use of security cameras will be to record images for future identification of individuals in the event of legal or policy violations. Legitimate safety and security purposes include, but are not limited to, the following:

1. Protection of buildings and property
2. Monitoring of Access Control systems
3. Verification of security alarms
4. Video patrol of public areas
5. Criminal investigation

F. Security cameras may be strategically placed to meet the specific needs of the District and college departments, and for the purpose of assisting the District Police Department to deter crime, manage emergency response situations, and investigate suspected criminal behavior.

1.2 DEFINITIONS

These definitions apply to terms as they are used in this procedure.

A. Centralized security system: Core infrastructure maintained by the Information Technology Department for purposes of storing and retrieving images from all security cameras deployed across the District. Infrastructure could include storage resources, such as disk drive arrays, as well as dedicated servers. Servers could perform activities such as storing images for later retrieval, retrieving images for investigation purposes, and maintaining logs of all access to stored security camera data.

B. Security camera: Any item, system, camera, technology device, communications device, or process, used alone or in conjunction with a network, for the purpose of gathering, monitoring, recording or storing an image or images of District facilities and/or people in District facilities for the purposes of enhancing public safety, monitoring restricted areas or equipment, to discourage theft and other criminal activities, and for preventing, investigating, and resolving incidents. Such devices may include, but are not limited to: analog and digital security cameras, close circuit television (CCTV), web cameras, and computerized visual monitoring.

C. Security camera data: Digital or analog Images captured or recorded by security cameras, which may be real-time or preserved for review at a later date.

D. Security camera systems: any electronic service, software, or hardware directly supporting or deploying a security camera.

E. Video Security Application: Any device or component that captures images for the purpose of deterring unlawful behavior or identifying the perpetrators of unlawful behavior. Images may be viewed immediately and/or kept on a storage device. Examples of video security applications include closed-circuit television (CCTV), video cameras, web cameras, and still cameras.

F. Web Camera – Camera utilizing TCP/IP (transmission control protocol/internet protocol) technology

1.3 POLICY

A. The purpose of security cameras in public areas is to deter crime and to assist the police and security personnel in protecting the safety and property of the District community. Any diversion of security technologies and personnel for other purposes (e.g., monitoring of political or religious activities, or employee and/or student evaluations) would undermine the acceptability of these resources for critical safety goals and is therefore prohibited by this procedure.

B. Use of cameras in public areas for security purposes will be conducted in a manner consistent with all existing District policies, including the Unlawful Discrimination Policy and Unlawful Harassment Policy. This procedure prohibits monitoring based on the characteristics and classifications contained in the Non-Discrimination Policy (e.g., race, gender, sexual

orientation, national origin, disability, etc.). Camera control operators will monitor based on suspicious behavior, not individual characteristics.

C. Security cameras will be used in a professional, ethical and legal manner, consistent with all existing District policies and local, state and federal laws and regulations.

D. Security cameras may be installed in situations and places where the security of either property or people would be enhanced. When appropriate, cameras may be placed campus-wide, inside and outside of buildings.

E. Unless the camera is being used for criminal investigations or for approved academic purposes, security cameras will not be used in areas where there is a reasonable expectation of privacy. Private areas include, bathrooms, shower areas, locker and changing rooms, areas where a reasonable person might change clothes, and private offices.

F. Information obtained through security recordings will only be released when authorized by the Chief of Police according to the procedures established in this procedure.

G. Departments currently managing their own system need to come into compliance with the administrative requirements of this procedure within six months.

H. The District Police Department reserves the right to review and approve any proposed or existing installation of video security applications on properties owned, leased, or controlled by the campus. All video security applications must conform to federal and state law in addition to District policy and procedure. All departments using security cameras are responsible for implementing and complying with this procedure in their respective operations. Video security applications must conform to standards established by the District so recorded data are easily retrievable. Nothing in this procedure prevents the use of video monitoring or observation in connection with an active criminal investigation or specific court order.

1.4 SCOPE

A. This procedure applies to all personnel, departments, and colleges of the District and 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. Although the physical cameras may be identical, the functions of these cameras fall into two 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, 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. In this case video may or may not be recorded. Example: a computer lab with multiple rooms and only one staff.

1.5 MONITORING AND ACCESS TO DATA

A. MONITORING

1. Under no circumstance will the District use camera technology to monitor specific staff, faculty, other academic personnel, students, vendors, contractors or other visitors work behavior unless there is a legitimate investigation pertaining to conduct contrary to the law or District policy. Any such monitoring or review must be accompanied by a written complaint, report, memo, email or any correspondence as to the nature, scope and level of action to be taken. The District will seek guidance from the District Police Department, Executive Vice Chancellor of Administrative Services, and, in all instances, legal counsel, to ensure legal and policy compliance.

2. Information obtained through video security applications will be used primarily for security and law enforcement purposes. However, the District may also use it in support of disciplinary proceedings against faculty, staff, or student(s), or in a civil suit against person(s) whose activities are shown on the recording and are the basis for the suit.

3. For property protection and personal safety cameras, access to live video or recorded video from cameras shall be limited to authorized personnel of the District Police Department and other persons authorized by the Chief of Police or designee. The copying, duplicating and/or retransmission of live or recorded video for extended responsibility cameras shall be limited to persons authorized by the Chief of Police or designee when the system was installed, or as updated in writing by the responsible department and accepted by the Chief of Police and college president.

B. ACCESS

1. District Facilities Planning and District Police Department staff will monitor system design to ensure systems are configured to reasonably prevent camera operators from tampering with or duplicating recorded information.

2. Video footage will be stored in a secure location and/or on servers accorded appropriate computer security with access by authorized personnel only.

3. Only the District Police Department may release data produced by video security applications. A list of people who can be contacted about the video security application during business hours and after hours, will be determined by the District Police Department.

4. When an incident is suspected to have occurred, designated personnel may review the images from security camera data.

5. 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.

6. Only authorized members of the District Police Department or the District's Internal Audit Department may review the results of the use of recording equipment. Other individuals who may have a legitimate need (in accordance with the law) to review the recorded material may be permitted to do so, but only with the prior approval of the Executive Vice Chancellor of Administrative Services.

   a. If it is determined that a crime or accident has occurred in an area where video recording may have taken place, then the recorded media shall be reviewed by authorized members of the District Police Department to determine if the incident has actually been recorded. If it is determined that the media does contain evidence of a crime, then that portion of the media will be maintained according to police procedures.

C. PUBLIC AND OTHER AGENCY REQUESTS

1. Any requests for recorded video images that come from non-CCCCD employees will be promptly submitted to the Executive Vice Chancellor of Administrative Services. Every reasonable effort should be made to preserve the data requested until the request has been finally processed by the District.

2. Public and media requests for video images captured by security cameras will be made available only to the extent required by law. In many cases, especially where a student is identifiable, a subpoena will be required.

3. Requests from District entities to release information obtained through security cameras must be submitted to the Executive Vice Chancellor of Administrative Services.

D. USE OF CAMERAS FOR CRIMINAL INVESTIGATIONS

1. The use of mobile or hidden video equipment may be used in criminal investigations by the District Police Department. 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 Chief of Police.

1.6 DATA RETENTION

A. Recorded images will be stored in a secure location with access by authorized personnel only. Designated police personnel from the District Police Department, and patrol officers conducting preliminary criminal investigations will have access to the video tapes/digital recordings.

B. In most cases, recorded video media will be stored for a period of not less than 30 days and will not exceed 60 days. This is based on configuration settings in the recording device. At that point, stored images to a hard drive will be re-written and unavailable. An exception to this procedure is video retained as part of a criminal investigation or court proceeding (criminal or civil), or other bona fide use as approved by the Executive Vice Chancellor of Administrative Services. Images saved for such purposes may be recorded to a DVD or other multimedia storage device in accordance with applicable evidentiary law. For each approved recording

system, a clear retention schedule shall be established as part of the approval process and must be adhered to very strictly. All recorded media must be stored in a secure location, the nature of which must be identified as part of the approval process.

C. Security records shall not be stored by individual departments.

D. No attempt shall be made to alter any part of any security recording. Security centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.

1.7 CAMERA REQUESTS AND INSTALLATION PROCEDURES

A. Camera Placement and Equipment Type

1. The decision to deploy security cameras and the specific placement of those cameras falls under the authority of the Chief of Police. The Chief of Police will base decisions on mitigating risks, vulnerabilities and historical acts of criminal behavior. When developing strategies for camera installation and placement, the Chief of Police will refer to the Districtwide Security and Access Control Standard.

2. This information is also critical in determining the types of equipment most appropriate for each situation. These factors might determine such outcomes as; Pan, Tilt Zoom (PTZ) cameras, fixed cameras, color, night, day/night cameras, etc.

B. Installation of video security applications and equipment are the financial responsibility of the requesting department. This responsibility includes the cost of IP addresses, service, and maintenance. ***(Fees are subject to approval by each individual campus budget office)*** Departments wishing to install or use security cameras are responsible for the purchase of all necessary equipment including cameras, wiring, servers, and software. The departments are responsible for the upkeep of the security cameras and recording systems they purchase. Departments purchasing security cameras and recording systems shall designate at least one "Departmental Contact Person" as the main contact for technical and day-to-day operations of the security cameras purchased. When technical problems are observed by the Police Department, they shall report them to District IT.

C. Any video recording software purchases made after January 1, 2015, must be approved by the District IT Department to meet a specific software standard. The software standard can be obtained through the IT Department or the Facilities Planning Department.

D. No audio shall be recorded except in areas where no one is routinely permitted. Requests to utilize audio surveillance that does not comply with this requirement will be evaluated on a case by case basis by the District Chancellor's Cabinet and legal counsel.

E. Individual colleges, departments, programs, or campus organizations installing video security equipment shall submit a written request to their appropriate dean or manager describing the proposed location of security devices, justifying the proposed installation, and identifying the funding source or sources for purchase and ongoing maintenance.

F. The vice president, dean or designee will review the request and recommend it to the Chief of Police or designee, if appropriate.

G. The Chief of Police will review all proposals from deans and vice presidents and will forward the proposal to the District Chancellor's Cabinet with a recommendation.

H. The District Chancellor's Cabinet will be responsible for reviewing and approving or denying all proposals for security camera equipment recommended by the Chief of Police

I. The IT Department shall oversee the installation of all approved security camera systems with the assistance of the District Police Department, and Facilities, as required.

J. At least five business days notice must be provided to District Information Technology Department prior to changing an IP address for a video system.

K. All existing security cameras that are not connected to the District's centralized security system must submit a Security Camera Location Document ***(another document to create)*** to the Chief of Police.

L. The District Police Department may establish temporary or permanent security cameras in public areas of the campus.

1.8 NOTIFICATION REQUIREMENTS (SIGNAGE)

A. All locations with security cameras will have signs displayed that provide reasonable notification of the presence of security cameras. At a minimum this must include primary building entrances. All proposals for the deployment of security cameras will include proposed sites for the placement of notifying signs. The placement of the signs and the text on the signs will be subject to the review and approval of the Chief of Police.

B. Conspicuous public signage must be displayed at all camera locations or the entrance to a single facility, except at emergency or investigative locations. Security installations may or may not be monitored continuously. Therefore, departments with active security camera installations must post signage stating, "This area is subject to video monitoring for security purposes and may or may not be monitored."

1.9 TEMPORARY SECURITY CAMERAS

A. From time to time and for various reasons, it may be appropriate to temporarily install video devices on campus (for example, in the course of police investigations in areas of the campus where thefts or breaches have been noted). To ensure individual privacy rights are protected in accordance with the law during the temporary installation of recording equipment for monitoring or for observation purposes, the following procedures must be followed before such devices may be temporarily installed anywhere on campus:

1. To the extent possible, the District Police Department will coordinate the use of portable video recording devices with the designated users of the space involved (for example, dean, department chair, or other District administrator). This procedure acknowledges, however, that this may not always be possible, given the nature of investigations that may be undertaken by the District Police Department.

B. Mobile or portable video equipment may be used in criminal investigations, however, this equipment will only be used in non-criminal investigations where there is significant risk to public safety, security and properly authorized by the Chief of Police.