UC SANTA BARBARA
POLICY AND PROCEDURE

Video Cameras and Video Surveillance
Contact: Chief Information Officer
Issued: _____, 2020
Pages: 9

VIDEO CAMERA AND VIDEO SURVEILLANCE POLICY

The use of Video Cameras helps deter crime, promote safety and security for people and property, and can benefit researchers and other members of the campus community in myriad ways. This Policy addresses installation and use of Video Cameras at UC Santa Barbara and seeks to address public safety concerns and community needs, while protecting individual rights and academic freedom.

I. SCOPE

This policy sets forth the requirements and standards for the installation and use of Video Cameras on all property owned, leased, or maintained by the University of California, Santa Barbara (UCSB), as well as the procedure for release of any images captured by Video Cameras on any property owned, leased, or maintained by UCSB. Video Cameras installed prior to the issuance of this policy are also subject to the standards and requirements set forth herein.

The following video applications are outside of the scope of this Policy:

- Delivery of education/training;
- Research Cameras that do not capture human images;
- Research Cameras that capture human images with the explicit consent of the human subject(s);
- Video recording medical procedures;
- Recording of artistic or creative performances;
- Recording of athletic events;
- Commercial television or movie recordings;
- Any mobile recording device used during the course of law enforcement, parking enforcement or transportation operations;
- Cameras designed to facilitate video conferencing; and
- Use of personal recording devices unrelated to official UC business.

II. POLICY

A. Definitions

Continuously Monitored Video Camera: A Video Camera, as defined below, that captures Video Data available for live viewing by a Camera Reviewer or, as appropriate, members of a specific department, or the public.

DVR Equipment: An electronic device used to record and store the Video Data captured by a Video Camera.

Dummy Camera: A decoy device deliberately designed and positioned to mislead an individual into believing an area is monitored by a Video Camera when it is not.

Private Spaces: Settings where an individual has a reasonable expectation of privacy and of being free from surveillance. This does not include a place where the public

has lawful access. The following are some examples of Private Spaces: residential living quarters, bathrooms, locker rooms, private offices, and designated lactation rooms.

Research Camera: A Video Camera, as defined below, used exclusively for the purposes of research conducted under the auspices of the UCSB Office of Research.

Sensitive Areas: Settings determined to be high risk and that require special protection. Examples may include: data centers, power facilities, facilities with secure requirements, and areas that house hazardous or controlled substances, museum collection or other displays of art, animal care facilities, any areas in which the exchange of currency or other forms of payment occur, and certain laboratory spaces.

Systems Operator: Any person charged with the operation and maintenance of a Video Camera. A Systems Operator may be a Video Camera Reviewer or any person or entity designated by a Campus Unit

Video Camera: Any equipment used to capture and/or record Video Data.

Video Camera Reviewer: The person or persons designated by a Campus Unit with authority to review Video Data in accordance with this policy.

Video Data: Visual images recorded by a Video Camera that can be viewed live, replayed, stored, and/or deleted.

Video Surveillance: For the purposes of this policy, Video Surveillance is Video Data collected for the purpose of detecting and promoting the security and safety of people and property at UCSB.

B. General Principles

Use of Video Cameras must be limited to applications that do not violate the reasonable expectation of privacy as defined by law and UC Policy. For additional information on how UCSB balances privacy and the appropriate use of Video Cameras for Video Surveillance or other applications, please see Appendix A: Privacy and the Use of Video Cameras on the UCSB Campus, as well as the UC Privacy Balancing Process.

Information obtained from Video Cameras must be handled with an appropriate level of confidentiality to protect against unauthorized access, alteration, or disclosure. Unauthorized access to, inadequate protection of, and inappropriate use, disclosure, and/or disposal of information obtained from Video Cameras must be immediately reported to the Video Camera Committee (VCCVCC) in accordance with the below outlined procedures.

Video Cameras must be maintained and fully functional in accordance with this policy.

Video Camera may only be installed, accessed, and used as outlined in this policy.

Appropriate Use

Video Cameras deter crime, assist in protecting University assets and in conducting research, and allow viewers to watch the surf at Campus Point or determine the crowd size at campus dining halls. However, Video Cameras must never by placed in Private Spaces or used for workforce monitoring or performance management of a UC Employee without approval by the VCC in accordance with Section IV.A of this policy. With the exception of Research Cameras and approved Continuously Monitored Video Cameras, information obtained from Video Cameras may only be monitored, reviewed, or otherwise used under the following circumstances:

1. When necessary to protect University community, buildings, and property;
2. When necessary to assist with the investigation of alleged illegal activity or suspected violation of University policy;
3. When necessary for maintenance or to verify the Video Camera is operating with full functionality pursuant to Section IV.E, below; or
4. When necessary to comply with legal obligations to preserve, release or otherwise use information.

Video Camera review must be conducted in a manner consistent with all existing University policies, including the Policy on Non-Discrimination.

Research Cameras

Research Cameras that capture human subjects without the explicit consent of the human subjects must be reviewed by the VCC. The VCC review is not intended as an approval process, rather a mechanism by which Research Cameras can be properly included in the VCC inventory and be subject to the requirements of this policy.

Continuously Monitored Video Cameras

In general, Continuously Monitored Video Cameras are approved only for locations where additional security is necessary, including but not limited to, areas of restricted access; retail/cash handling locations; as required by insurance or contract; in response to an alarm; special events; and specific police investigations. Continuously Monitored Cameras may also be approved, on a case-by-case basis, when it is apparent there is no expectation of privacy in the space captured by the Video Camera and members of a specific department or the public may access the Video Data recorded by such camera.

C. Prohibited Use

Video Cameras must not be located in places where a person has a reasonable expectation of privacy. Video Cameras may not be located in the following places without a court order: residential bedrooms, bathrooms, or locker rooms.

When reviewing Video Data, Video Camera Reviewers must evaluate such data for suspicious behavior, not individual characteristics such as race, gender, ethnicity, sexual orientation, or disability.

Video Camera systems must not record audio unless prior approval is obtained from both campus General Counsel and the VCC.

Dummy Cameras are prohibited.

Deliberately hidden Video Cameras are prohibited, unless specifically authorized in advance as part of a police investigation and with prior approval of the VCC in coordination with Campus Counsel.

Video Cameras personally purchased and/or owned by faculty, staff, or students may not be installed for official University business.

D. Storage and Security

Video Data from Video Camera systems must be secured and configured to prevent unauthorized access, modification, duplication, and/or destruction, in accordance with the standards set forth by the VCC.

Video Data from Video Cameras must be retained in accordance with UC Policy and securely overwritten or destroyed in accordance with the UC Records Retention Schedule.

Suspected unauthorized access or tampering with a Video Camera or Video Data must be reported to the VCC immediately upon discovery. Report unauthorized access via Service Now under Information and Technology Services.

E. Release

Submit all requests for release of Video Data to anyone other than the UC Police Department and the Video Camera Reviewer(s) authorized to review Video Data recorded by the Video Camera in question, to the VCC for review and approval.

Requests for release of Video Data may be made via Service Now under Information and Technology Services.

Video Data may only be released if it will be used and retained in a secured environment. Video Data shall be released to the fewest individuals necessary.

The VCC shall not authorize the release of Video Data unless the release is under one or more of the following circumstances:

1. **Public Convenience**: The information from the Video Camera is being captured for public convenience purposes (e.g., the cameras that monitor or record building construction/renovation progress, traffic, weather), as documented in the proposal approved by the VCC.
2. **Explicit Consent**: All individual(s) depicted provide explicit consent to release.
3. **Research Release**: Video Data may be released to a principal investigator for conducting research. Research proposals must be approved by the VCC in coordination with Campus Counsel and the Human Subjects Committee.
4. **Internal Investigatory Release**: Video Data may be released to an official University investigator if necessary to investigate alleged illegal activity or a potential violation of University policy.

5. Personnel Action: Video Data may also be released to a University employee, where that employee is, or may be, subject to personnel action on the basis of such Video Data as well as to the employee's representative and to the University's representative in connection with the administration of such a personnel action.
6. External Release: Video Data may be released to a UC non-affiliate if necessary to either: (1) Investigate incidents or accidents; or (2) Comply with legal obligations to preserve, release or otherwise use information, including requests under the California Public Records Act and all subpoenas, warrants, court orders, and other legal documents directing that access be afforded to external law enforcement agencies. Prior to releasing Video Data, the non-affiliate must agree to secure the information and limit redistribution. Both the VCC and UCSB Campus Counsel must review and approve all requests for the release of information from Video Cameras to an external user.

The VCC must keep a log of all instances of release of information from Video Cameras.

III. RESPONSIBILITIES

Chief Information Officer: The Chief Information Officer (CIO), or designee, shall be responsible for:

1. Monitoring and reporting compliance with this policy; and
2. Campus Video Surveillance content integrity and the prevention of misuse of Video Data.

Chief Information Security Officer: Member of the VCC and responsible for answering any questions regarding video security and safety.

Video Camera Committee: Reporting to the Chief Information Officer, the VCC will provide strategic oversight of Video Surveillance on campus and is responsible for:

1. Approving Video Camera installation, use, and decommissioning in accordance with this policy;
2. Evaluating all requests for the release of Video Data to anyone other than the UCPD or a Video Camera Reviewer, in accordance with this policy;
3. Establishment and oversight of an annual certification process by which all Campus Units will be required to certify that each Video Camera owned and operated by that unit is operational and secure.; and
4. Tracking and inventory of all approved Video Cameras on campus.

The VCC is guided by the University of California Privacy Principles and Values and must monitor developments in law and the security industry to ensure that campus' use of Video Cameras is consistent with best practices and must propose and review appropriate changes to this policy, as well as to any standards or procedures established by this committee, as needed.

At minimum, the VCC shall be comprised of the Campus Privacy Official, the Chief Information Security Officer, and a member of the UCPD. The CIO may appoint additional representatives as necessary.

Campus Unit: For the purposes of this policy, the definition of a Campus Unit includes individual colleges, departments, programs, or campus organizations. All Campus Units installing and using Video Cameras are responsible for implementing and complying with this policy and the procedures set forth in Section IV below. The Campus Unit must designate an administrative official (such as a Dean, Director, or Manager) as a Video Camera Reviewer.

Video Camera Reviewer: Video Camera Reviewers designated by the Campus Unit, and approved by the VCC, are authorized to view Video Data. Video Camera Reviewers must:

1. Perform their duties in accordance with this policy and the scope of use approved by the VCC in the Video Camera proposal; and
2. Provide written acknowledgement that they have read and understand this policy.

Campus Privacy Officer: Member of the VCC and responsible for the tracking and recording of all approvals for release of Video Data.

Systems Operator: Responsible for ensuring a Video Camera is operational with full functionality and for conducting required maintenance in accordance with this policy.

IV. PROCEDURES

A. Approval

A Campus Unit must obtain prior approval from the VCC before installing or implementing a significant change to a Video Camera system.

A significant change that requires VCC approval includes, but is not limited to, the following:

- Changing the area monitored by the camera;
- Changing a camera from one that is not continuously monitored to one that is a Continuously Monitored Video Camera; or
- Changing the Campus Unit responsible for the camera.

To obtain approval to install a Video Camera, or implement a significant change to an existing Video Camera, a Campus Unit must submit an online application to the VCC via Service Now under Information and Technology Services.

The VCC is responsible for conducting a review of the Video Camera application for compliance with this and other campus policies. The VCC will consult with other departments on campus, such as General Counsel and Risk Management, when reviewing Video Camera applications, as necessary.

Video Camera applications for installation in areas of campus where there is no reasonable expectation of privacy may be approved by the VCC without stakeholder consultation. However, when the VCC receives an application for a Video Camera installation in an area where there may be an expectation or limited expectation of

privacy, the VCC will consult with representatives from the Academic Senate, Office of Student Life, Graduate Student Association, Associated Students, Human Resources, and/or University Administration, as appropriate. These representatives will have 45 days to review the application with their stakeholders and submit comments to the VCC. The VCC must review the comments from the stakeholders and make modifications as necessary to the application before granting final approval. If stakeholders make no comments, the VCC will move forward with approval at the end of 45 days.

The VCC will notify Labor Relations of proposed Video Camera installations to ensure represented employees receive proper notice.

In the event of an emergency, the VCC may expedite the review and approval process. In such circumstances, the Campus Unit must obtain written approval from the VCC prior to the deployment of the camera equipment. Emergency approval by the VCC shall be made in coordination with Campus Counsel. A full application must be submitted, and notifications made to interested parties, as soon as possible.

The VCC must maintain documentation of approved applications in accordance with the UC Records Retention Schedule.

Video Cameras installed, or that undergo a significant change, without prior approval from the VCC are subject to removal, without notice, by university personnel authorized by the VCC.

B. Approval of Previously Installed Video Cameras

Within 90 Days of this issuance of this policy, any Campus Unit that installed a Video Camera prior to the date of issuance of this policy must submit an application to the VCC to obtain approval for the continued use of that Video Camera. Continued use of the Video Camera will not be approved unless the Video Camera and its maintenance and operation are in conformity with this policy and the procedure outlined herein. Video Cameras not in compliance are subject to removal as Dummy Cameras. However, prior to removal, the VCC must make every effort to try to determine ownership of the Video Camera, and attempt to work with the Campus Unit to resolve compliance issues.

C. Procurement and Installation of Cameras

After having received approval from the VCC to proceed, departments must procure camera equipment in accordance with campus and UC policy. Installation of Video Cameras and DVR Equipment must be in accordance with applicable campus policies. All installations must conform to any requirements imposed by the VCC.

Applications for Video Camera installation and changes must conform to the campus technical standards as set forth by the VCC in accordance with law and UC Policy. Equipment that does not meet this standard must be reviewed for approval on a case-by-case basis by the VCC.

The VCC is responsible for developing and maintaining a master inventory to track installations of approved Video Cameras. Video Camera installations made prior to this policy shall be incorporated into the master inventory. Minimum data elements required for the inventory are in Appendix B.

D. Signage

Signage indicating the presence of cameras shall be created, placed, and installed in accordance with the specifications set forth by the VCC upon their approval of the camera's installation.

Video Cameras without conspicuous signage may be reported to the VCC via Service Now under Information and Technology Services.

Video Cameras installed without proper signage, in accordance with the specifications set forth by the VCC, are subject to removal, without notice, by university personnel authorized by the VCC.

E. Operation and Maintenance

Campus Units with Video Cameras must maintain a list of all authorized Video Camera Reviewers. Only those individuals on the list of authorized Video Camera Reviewers may access Video Data obtained from the Video Camera.

Campus Units must maintain and test their Video Camera(s) monthly to verify proper operation and full functionality. If a Video Camera is not operative or fully functional to original design specifications, the Video Camera must be repaired within 30 days. Cameras not repaired within 30 days are subject to removal as Dummy Cameras. Annually, Campus Units must certify to the VCC that all Video Cameras in their Campus Unit are operational and fully functional to original design specifications. Video Cameras will be subject to periodic audit by Audit and Advisory Services to ensure compliance with this policy.

System Operators may incidentally access live and recorded Video Data to ensure the proper operation and security of the Video Camera System. Such operators are not authorized to disclose what they incidentally observe except as required by policy or law.

Campus Units with Video Cameras must provide Video Camera Reviewers with appropriate work facilities so unauthorized persons cannot view the Video Data obtained from Video Cameras.

Video Cameras that are no longer functional or in use must be decommissioned in accordance with Section IV.F of this policy.

F. Decommissioning a Video Camera

When a Video Camera is no longer in use or needed by a Campus Unit, the Campus Unit shall apply online to the VCC to decommission the Video Camera via Service Now

under Information and Technology Services. Upon receipt of the decommissioning request, the VCC will issue a decommissioning process to the Campus Unit.

The VCC must maintain documentation of the decommissioning of Video Cameras in accordance with the UC Records Retention Schedule.

G. Reporting a Suspected Violation of Policy or Criminal Activity

Suspected Policy Violation

When a Campus Unit believes a camera may have captured evidence of a policy violation that may warrant disciplinary action, the Campus Unit shall report their findings to the applicable unit head. No one, other than approved Video Camera Reviewers may review the Video Data in question.

If the applicable unit head determines that an investigation is appropriate, the applicable unit head must submit a request for release of the video data to the VCC in accordance with Section II.F of this policy.

Upon receipt of the request for release, the VCC will determine whom, if anyone, may access the Video Data for investigatory purposes. To determine whom the Video Data will be released, the VCC will consult with the appropriate administrative offices such as Human Resources, Academic Personnel, Student Affairs, and/or Campus Counsel.

Suspected Criminal Activity

When a Campus Unit believes a camera may have captured evidence of criminal activity, the Campus Unit shall report their findings to the UCPD to review information obtained from the Video Camera system. Campus Units must permit the UC Police Department access to information obtained from the Video Camera system for investigations.

H. Exceptions

Requests for exceptions to this policy or the standards or procedures set forth by the VCC shall be made in writing to the VCC at vcc@ucsb.edu. The VCC must review all requests for exceptions in consultation with the CIO and Campus Counsel.

V. REFERENCES and RELATED POLICIES

BFB-BUS-43: Materiel Management
BFB-BUS-80: Insurance Programs for Institutional IT Resources
Defacement of Interior Surfaces
Implementation of Electronic Communications Policy
Electronic Communications Policy (Systemwide)
Policy on Non-Discrimination
UC Privacy Balancing Process
UC Privacy Principles and Values
UC Records Retention Schedule

Appendix A:
PRIVACY AND THE USE OF VIDEO CAMERAS ON THE UCSB CAMPUS

The Video Camera and Video Surveillance Policy is guided by Fourth Amendment protections and seeks to balance UCSB's right and need to conduct video surveillance to protect property and persons with the privacy rights of the faculty, staff, students, and visitors on the UCSB campus.

When considering whether to approve the installation of a Video Camera in a particular location, the VCC considers, among other things, one primary question: Is there a reasonable expectation of privacy in the proposed location?

In California, it is generally reasonable to expect that a locker room and bathroom are private. On the other hand, parking lots, most outdoor areas, public lobbies, and conference rooms are public and one's expectation of privacy is minimal.

Whether an individual's office or a particular hallway is "private" may be dependent on a number of factors, including public access to the area in question. If anyone can enter the space, it is likely a public space with little or no reasonable expectation of privacy. However, some interior corridors may be private because the building and/or hallway are accessible only by a small number of individuals. In this type of semi-public/semi-private area, the expectation of privacy is limited.

As members of the University of California, the faculty, staff, and students at UCSB generally have a greater expectation of privacy than the general population. Therefore, when a Video Camera is installed in a semi-private space, individuals with access to that space (such as faculty with offices) may consider the installation invasive of their privacy. On the other hand, Video Camera installations to monitor expensive research equipment, such an installation may be welcome. The VCC balances these privacy interests to determine whether to approve an application for the use of a Video Camera.

As part of this balancing test, and in addition to the reasonableness of privacy expectations, the VCC also considers:

1. The purpose for the video surveillance.
2. What the camera will capture in its scope of view. Will the camera capture computer screens, telephone keypads, part or all of a particular space?
3. How long the camera will be in place.
4. Who is requesting authorization to have access to the video data?

The Video Camera and Video Surveillance Policy ensures that:

1. Only authorized individuals with appropriate training have access to recorded video data;
2. Video data is released in strict accordance with law and policy;
3. The installation and use of Video Cameras is in conformity with law and policy; and
4. All individuals whose image may be captured by a Video Camera on the UCSB campus be given proper notice.

Appendix B:
DATA ELEMENTS REQUIRED FOR VIDEO CAMERA INVENTORY

The following data elements are required for each Video Camera installation for inclusion in the campus Video Camera inventory:

- Department
- Location (description)
- Intended use (purpose)
- Description of view
- Planned operation duration
- Continuously monitored y/n
- Audio y/n
- Primary camera reviewer
- Secondary camera reviewer
- Approval date
- Decommission date
- Fault detection capability of camera
- Maintenance and repair responsibility and contact