Ohio Administrative Code

Rule 3344-76-01 Closed circuit television.

Effective: June 4, 2016

(A) Purpose

(1) Cleveland state university (CSU) holds the security and safety of individuals on campus as one of the utmost concerns. Closed circuit television (CCTV) security surveillance is an important tool to assist keeping individuals, property, and research as safe as possible.

(2) This rule regulates CCTV use and related systems for necessary system compatibility, standardization, image quality, restrictions, and responsibility.

(3) The access control and security systems department (AC&SS) may issue procedures, protocols, manuals, forms, and other detailed operational processes to implement this rule.

(4) This rule applies to all faculty, staff, students, affiliates, auxiliary organizations, contractors, and suppliers who are or become involved with a CCTV device or related need at CSU.

(B) Rescission of other guidance

This rule replaces and supersedes any previous CCTV-related guidelines, protocols, understandings, and/or similarly intended documents or practices.

(C) Compliance

(1) All members of the university community (students, faculty, staff, affiliates, etc.), those doing business with or at the university, and those on university-controlled property must fully comply with this rule. Failure to comply could result in discipline, loss of CCTV access privileges, or legal action.

(2) Any company contracted to manage a CSU-related facility, including a residence hall(s), must

abide by this rule, maintain university AC&SS CCTV standards, contractual agreements, and any written or verbal instructions from the AC&SS department related to CCTV.

(3) Any perceived use of CCTV systems not in accordance with this rule must be reported to the manager of AC&SS for compliance correction.

(D) Responsibilities

(1) The manager of AC&SS has the responsibility for determining proper security-related measures, hardware, and software for any CSU-related facility, including the documentation and licenses for the systems and equipment needed to maintain AC&SS standards. All aspects of CCTV (equipment, maintenance, system design, placement, views, installation, pre-sets, use, etc.) are under the direction and authority of the AC&SS department.

(2) After a device or system is online and functional, AC&SS is responsible for the transmission of images from the camera to the local recording device (DVR, NVR, SVR, etc.). The CSU information services and technology (IS&T) department is responsible for secure transmission of images/data from the local recording device to the mass storage device and other approved locations.

(E) Coverage

(1) The intent of CCTV coverage on campus is as a security tool to deter crime and provide a historical record of covered incidents. Security technologies and personnel may not be used for other purposes, such as the intentional monitoring of students or employees.

(2) During the design phase for new CCTV installations, the manager of AC&SS will meet with the building's representative or funding sponsor and a designated university police representative to explain the CCTV design and obtain feedback for any potential adjustment the manager of AC&SS deems appropriate. Once a plan is approved by the manager of AC&SS, any deviations from the plan must be approved by the manager of AC&SS and updated on the construction plans by the contractor.

(3) The manager of AC&SS will select camera positions, angles, views, and pre-sets with the ability

to change a view based on a change in environment or need. At least once a year, the chief of police will designate a representative to review existing camera views for potential need for adjustment.

(4) CCTV installation will not occur in areas where there is a reasonable expectation of privacy, such as: inside restrooms, inside locker rooms, inside dressing rooms, and similarly situated spaces.

(5) Covert camera use and recordings will only be used to aid in criminal investigations by the university police department. Approval of such use must be approved by the university police through the manager of AC&SS.

(F) Image and footage availability

(1) Generally, security camera images and feeds are not live-monitored by any individual, but all camera images are intended to be recorded on a twenty-four hour basis every day of the year. Lighting conditions, equipment quality, and a camera's custom trigger parameters may affect image availability. Live and recorded images are available to the university police and AC&SS. Access by others to any camera image or feed must be approved by the manager of AC&SS.

(2) Unauthorized access or distribution of any camera image is strictly prohibited without the express written permission of the manager of AC&SS. Any violation is considered a serious violation of university policy, and is subject to the full extent of university discipline, potential criminal charges and legal action.

(3) The university's goal is to retain recorded images for thirty days; however, there are numerous factors that can limit the retention significantly on a specific camera's recorded history. Requests to review or be provided recorded CCTV images should be made immediately upon identifying the potential need.

(4) Requests for access to review or release CCTV images that are not required for university business or law enforcement purposes shall be made to the office of general counsel in accordance with CSU's public records request procedures.

(5) Review of footage to investigate potential employee misconduct requires pre-approval from the

assistant vice president of human resources; any use of CCTV footage specifically for the purpose of investigating employee misconduct must conform with applicable CSU policies and, for employees who are members of a collective bargaining unit, the terms of any applicable collective bargaining agreement.

(6) Video or images used for criminal investigation purposes by the CSU police or requested by other law enforcement agencies having jurisdiction is not subject to the CSU public records request procedures. AC&SS staff will make every effort to assist the requesting agency in quickly obtaining video as needed to aid in the apprehension of a person who has committed a crime or the prosecution of criminal activity. In circumstances where, based on a determination by the director of campus safety in consultation with the office of general counsel, an immediate threat to health or safety of the campus community exists, video shall be made available to law enforcement immediately.

(7) For a major security or safety incident, the manager of AC&SS will take all actions necessary to preserve related CCTV footage.

(G) Fees

(1) AC&SS will provide at no cost to university entities regular maintenance and reasonable repair (excluding abuse) of existing CCTV equipment and systems as funding and staffing allow.

(2) For non-maintenance related service, costs will be payable by the requesting or responsible entity based on the actual cost of the item (if any) and labor. Non-maintenance items or service may include, but is not limited to:

(a) Upgrading equipment

(b) Extensive repairs

(c) Replacement of outdated equipment

(d) Installation of new equipment

(e) Projects

(3) In relation to a public records request, provision to a requestor of CCTV images or footage on a removable medium will be provided at the cost of the medium. The manager of AC&SS will provide an approximate estimate of costs prior to fulfilling an approved request.

(H) Code of practice

Authorized viewers of CCTV images or feeds will adhere to the following "Code of Practice":

(1) Viewers will not monitor individuals solely based on characteristics of race, gender, ethnicity, sexual orientation, gender identity, gender expression, disability, or other classifications protected by the university's non-discrimination policy.

(2) Viewers will not zoom-in or continuously view people becoming intimate in public areas.

(3) Viewers will not zoom-in on any portion of a person other than for purposes of determining an action taking place, identification, training, or testing of equipment.

(4) Viewers will not zoom-in into offices or residential rooms unless a potential incident is in development and such camera control is authorized by the university police officer-in-charge (OIC) or senior campus safety management.

(5) A violation of the code of practice is subject to disciplinary action consistent with the rules and regulations governing members of the university community.

(6) The manager of AC&SS will maintain a list of all authorized viewers of any camera.

(I) Installation

(1) It is the responsibility of the manager of AC&SS and the university architect's office to ensure that this rule and the university's master security plan are provided and accepted by any general contractor or project principal that will be involved in the installation of CCTV-related equipment or

systems. Any suspected non-compliance must be reported to the manager of AC&SS for corrective action.

(2) Installation or repair of any camera or image recording device must be performed by a qualified individual that has been approved by the manager of AC&SS. Contractors shall schedule service with the AC&SS video unit prior to doing work on campus.

(3) For a contracted installation, AC&SS staff is neither the project managers, nor expected to supervise an installation. As the customer representing the university, AC&SS will pre-approve of the design, equipment, installation locations, and operation of the device/system, with the expectation that the contractor/installer will deliver a turn-key fully operational device and/or system with a fully functional tie-in to the university's existing enterprise-level video system. The manager of AC&SS, university architect's office and information services and technology will ensure that university standards are complied with.

(4) Individuals having knowledge of the installation details and operation of CCTV equipment and systems shall keep the information confidential. Any questions or concerns regarding installation work or operations must be directed to the manager of AC&SS.

(5) Regardless of the intended use, unauthorized fixed-mounted or stationary cameras, pan-tilt-zoom cameras, webcams, or other image capturing devices for personal or work-related use may not operate on CSU property without the written consent of the manager of AC&SS. Violators are subject to university discipline and legal action.

(6) Non-security related video equipment that may be approved at the discretion of the manager of AC&SS include, but are not limited to:

(a) Construction project progress

(b) CCTV system for research or academic purposes

(c) Training purposes

(d) Distance learning labs

(7) For CCTV equipment approved for use, the manager of AC&SS may require appropriate signage be publically posted notifying of the potential use of live or recorded video and/or audio.

(J) Plans and drawings

(1) All installed equipment and its related parts will be compatible with the existing enterprise-level security/video system at CSU, and plans/drawings will be provided by the contractor to the manager of AC&SS for approval before work begins. In the design phase, AC&SS will denote specific equipment placement and type. No plan deviation, alterations, or substitutions may be made without the consent of the manager of AC&SS.

(2) AC&SS will maintain a log of all camera equipment on campus. New installations by a contractor require pre-installation prints approved by AC&SS, and "as built" prints to AC&SS within ten days of project completion.

(3) For security purposes, all plans, drawings, and related information are designated confidential. No release of information is allowed without the consent of the manager of AC&SS. Violators are subject to university discipline, potential criminal charges and legal action.

(K) Equipment selection

(1) All new installations will utilize AC&SS-specified cameras and AC&SS-specified recording devices.

(2) This equipment is defined in the standards published by the office of the university architect. With the growth of the industry, specific equipment brand/model may be updated by the AC&SS video unit during the design/planning phase of the specific project.

(L) Tests

(1) An installer is expected to deliver a turn-key fully operational device and/or system with a fully

functional tie-in to the university's existing enterprise-level system. The contractor/installer must be present during a scheduled final acceptance test by the AC&SS department. The manager of AC&SS must approve and sign-off on any device/system prior to its acceptance.

(2) For existing equipment, the AC&SS department will maintain a log indicating the last test of each camera and recorder.

(M) General prohibitions

General prohibitions include, but are not limited to:

(1) Disabling or tampering with any university security device or security monitoring device, including CCTV equipment.

(2) Unauthorized access or use of CCTV software or systems.

(3) Physically relocating or re-positioning a fixed-lens camera.

(4) Covering or otherwise obstructing the lens of any camera.

(5) Installation or use of CCTV or any type video-capture equipment not pre-approved by AC&SS.

(6) Failure to comply with the university's master security plan relating to CCTV.

(7) Authorizing or utilizing non-AC&SS staff for any type of service related to CCTV security equipment or systems.

(N) Exceptions and appeals

(1) If an individual or entity believes that application of this rule will adversely impact the individual or entity, they must submit a written request for a specific exception to the manager of AC&SS within fifteen days of the date they were affected. The manager of AC&SS may or may not grant an exception based on the best interest of the university.

(2) Denial of an exception may be appealed in writing to the director of campus safety, who is the final decision authority. The response to the individual/entity will be within thirty business days of receipt.

(3) Requests for an exception or appeal must state at least the following:

(a) Name of affected individual and associated entity

(b) Contact information (mailing address, e-mail address, phone)

(c) The provision of this rule that is in question

(d) How the provision adversely affects the requestor

(e) Proposed remedy

(f) Information regarding previous attempts to resolve the issue.