



Ohio Administrative Code Rule 3337-44-119 Video surveillance systems.

Effective: January 22, 2018

(A) Purpose

This policy regulates the installation and use of video surveillance systems for safety and security purposes in public and semi-public areas on the Athens campus of Ohio university. This policy does not imply nor guarantee that surveillance cameras will be monitored in real time.

To ensure the protection of individual privacy rights in accordance with the law, as well as to preserve academic freedom and avoid discouraging the exercise of first amendment rights, this policy is adopted to formalize procedures for the installation of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance recordings.

Video surveillance will be conducted in a professional, ethical, and legal manner. Any diversion of surveillance records for other purposes (e.g., surveillance of political or religious activities) is prohibited. Under no circumstances will the contents of any video recordings be exploited for purposes of profit or commercial publication, nor will such recordings be publicly distributed except as may be required by law.

(B) Scope

(1) Public and semi-public areas

This policy applies to video surveillance in areas that are public or semi-public, in which there is not a reasonable expectation of privacy. It is important to note that just because an area may have restricted access, that alone does not create an expectation of privacy (e.g. residence hall lounges, computer labs, classrooms limited to students of a particular college or class, etc.)

(2) Private areas



Areas on campus that have a reasonable expectation of privacy, including classrooms, are prohibited from being subject to video surveillance under this policy. Generally, private areas on campus include, but are not limited to, classrooms, private living quarters, residential hallways, restrooms, single occupancy offices, etc. Normally, video cameras in areas that could potentially capture both private areas (e.g. a window into a residence hall room) and public or semi-public areas should be installed such that the cameras view does not include the private area. If reasonable measures cannot be taken to exclude private areas from a cameras view, the private areas will be digitally blocked from view on both live and recorded images.

(3) Exceptions

The following uses of video surveillance are exempt from this policy:

- (a) Criminal investigations conducted by or in conjunction with the Ohio university police department;
- (b) Academic instruction or feedback, as long as the video is not set to continuously record;
- (c) Public web streaming video in areas that do not have a "reasonable expectation of privacy" and are not recorded (e.g., on the Ohio university website);
- (d) Recording of public performance events for public entertainment (e.g., athletic events, plays, lectures, etc.).

(C) Procedures

- (1) OUPD has the exclusive authority to administer this policy.
- (2) All installations of video surveillance systems covered by this policy will use only the enterprise video surveillance solution chosen by the university.
- (3) OUPD, along with the assistance of design and construction and the office of information technology will oversee the installation of approved video surveillance equipment.



- (4) Video surveillance footage will only be recorded to the university's centralized server.
- (5) Appropriate signage will be placed at all locations under video surveillance. Signage will state, "This Area is Subject to Video Surveillance." Signage will also include contact information for the Ohio university police department.
- (6) Units responsible for the space in which a video surveillance system is being proposed will:
- (a) Draft a written request to the chief of police, or their designee, which includes:
- (i) Draft drawings which show the proposed location and direction of each camera;
- (ii) An employee who will be the unit's point of contact for the system; and
- (iii) Approval from the appropriate administrative head of the unit seeking the installation.
- (b) The chief of police, or their designee, will review the request for conformity to this policy and approve or deny the request.
- (i) If the chief of police, or their designee, intends to approve a request for video surveillance installation, he or she shall notify the chairs of the administrative, classified, faculty, and student senates and provide them with a copy of the approved request.
- (a) The chairs of the senates will have fourteen (14) calendar days from receipt of the notification of pending approval to object to the installation.
- (b) Objections will be filed with the vice president, or their designee, of the division in which the proposed installation falls and copied to the chief of police or their designee.
- (c) The appropriate vice president shall have final authority to resolve objections and notify the chief of police, or their designee, and the chair of the objecting senate of their decision.



(d) Once final approval is received, or if no objection is filed within fourteen calendar days of notification to the chairs of the senates, the chief of police, or their designee, shall notify the proposing unit of the installation's approval and the project may proceed.

(ii) If disapproved (either by the chief of police, or their designee, or as a result of an objection sustained by a vice president), the chief of police, or their designee, will notify the proposing unit and may include recommendations to bring the proposal into alignment with the policy. The unit may elect to make those changes and resubmit the proposal to the chief of police, or their designee.

(D) Use of video surveillance systems

(1) Video surveillance of public and semi-public areas will be conducted in a manner consistent with all university policies. Any perceived violation of university policy shall be resolved in accordance with applicable dispute resolution processes outlined elsewhere in university policy.

(2) OUPD will oversee access to the university's video surveillance system and to all video cameras individually. Real-time and historical video access will be restricted. At no time will access be granted to the system for the purpose of searching for unprompted evidence of wrongdoing.

(3) No video recordings will be duplicated without permission from OUPD.

(4) Real-time video access

(a) Any individual or department with a need to view video in real time will submit the form "Request for Real Time Video Access" to the chief of police, or their designee.

(b) The chief of police, or their designee, will review the request for a legitimate operational need and will approve or deny the request. If approved, OUPD will ensure access is granted.

(5) Historical recordings

(a) Agencies outside of Ohio university may need to obtain a subpoena for video recordings, as determined by the office of legal affairs.



(b) Historical recordings will be made available to Ohio university officials conducting bona fide investigations. The investigating official will submit the form Request for Historical Video Access to the chief of police, or their designee.

(c) The chief of police, or their designee, will review the request for conformity to this policy and will approve or deny the request as appropriate. If approved, the chief of police, or their designee, will ensure the investigating official obtains access to the recordings.

(i) Copies of recordings determined to have no administrative value will be returned to OUPD for destruction.

(ii) Copies of recordings determined to have administrative value will be retained by the investigating department, subject to their retention schedule policy.

(d) All Ohio university police officers and communications officers will have permanent access to all video surveillance systems, both in real time and historically.

(6) Any person who has been granted access to the video surveillance system will: (a) not allow their access to be used by another person; and (b) use their access only for the purpose of their job duties.

(E) Disposition of records

(1) No attempt will be made to alter any part of any video recording. Access to video surveillance systems will be configured to prevent tampering with records.

(2) Ohio university police department will determine the minimum standards for video recording.

(3) Video surveillance records on the central server, when recording at minimum standards, will be stored for a period not less than thirty days and will then promptly be deleted.

(4) If an operational need arises for a camera(s) to record above the minimum standard, the units point of contact or investigating official should submit a request in writing to the chief of police, or



their designee, explaining the need and duration for the change. Such requests will be approved or denied by the chief of police or designee. Due to data storage limitations, video recordings for the approved camera(s) may not be available for the full thirty day retention period. The chief of police or designee will ensure that the affected cameras are restored to minimum standards as soon as practical.

(F) Transition of legacy video surveillance systems

(1) Legacy video surveillance systems refer to those video surveillance systems that are subject to this policy, but were installed prior to the effective date of this policy and were not connected to the enterprise video surveillance system solution utilized by the university on the effective date of this policy.

(2) Legacy video surveillance systems will be transitioned to the university's enterprise video surveillance system by December 31, 2018. Video surveillance systems that are not transitioned to the enterprise video surveillance system by December 31, 2018 will be deactivated.

(3) Once transitioned, all video surveillance systems will be administrated, maintained, and operated in accordance with this policy.

The version of this rule that includes live links to associated resources is online at

<https://www.ohio.edu/policy2/44-119.html>