

3356-4-11 Closed circuit television system use.

- (A) Policy statement. To standardize the installation and regulate the use of closed circuit television (“CCTV”) and any other related surveillance systems at Youngstown state university in order to deter crime, enhance campus security, and assist the Youngstown state university police department (“YSU-PD”) in its response to safety and security issues on university property.
- (B) Definitions.
- (1) “Equipment.” Any item, system, technology device, or process, including software, used alone or in conjunction with a network for the purpose of gathering, monitoring, recording or storing an image, images, and/or audio. Images and/or audio may be viewed in real-time and/or captured and preserved for possible review at a later date.
 - (2) “Monitoring.” The process of observing or reviewing recordings that are captured by ~~eee~~CCTV equipment either in real-time or that have been prerecorded and are reviewed at a later date and time.
 - (3) “Recording.” The process of capturing images and/or audio using CCTV systems and saving those images to a storage medium.
 - (4) “University property.” All land, structures, or other real property owned, operated, leased or controlled by Youngstown state university. This includes both internal and external areas, including but not limited to common spaces, grounds, and parking lots.
 - (5) “Internet protocol (‘IP’).” The communication protocol used in the collection and transmission of recordings on the CCTV network. All surveillance devices shall utilize open internet protocols and standards.
 - (6) “Public areas.” Any portion of university property that is operated and controlled by Youngstown state university, including buildings and facilities, in which a person does not have a reasonable expectation of privacy.

(7) “Private areas.” Any portion of university property where a person would have a reasonable expectation of privacy, e.g., restrooms, residence rooms, personal offices, or locker rooms, or any other area designated as a clothing changing area. Personal offices do not include reception, informational or waiting areas.

(8) Restricted access areas. University property that is not accessible to the general public. Restricted access areas may be accessible to university employees, but do not include private areas.

(C) Parameters.

- (1) The YSU-PD is responsible for implementation of this policy, including the approval, placement, and monitoring of all CCTV surveillance systems (“CCTV system[s]”) on university property.
- (2) This policy does not apply to the use of video or visual surveillance, monitoring or recording, covert or otherwise, by the YSU-PD for criminal investigations or as authorized by a court of law.
- (3) This policy does not apply to the legitimate academic use of cameras or video recordings for educational or journalism purposes, the general use of webcams by the university, ~~or to~~ the use of video recording for public performances, events, or interviews, or for university academic or research purposes
- (4) This policy does not imply or guarantee that the CCTV system will be monitored in real time.
- (5) The CCTV system will be utilized in a professional, ethical and legal manner.

(D) Procedures.

- (1) Any and all requests for use of CCTV systems and/or equipment will be made in writing to the chief of the YSU-PD. The request will include the name of the college or department making the request, the purpose or reason for the request, and the desired

installation area. YSU-PD will review each proposal and ~~recommended specific equipment and installations or repositioning as dictated by institutional needs and current technological standards.~~ ~~The~~ the review will consider security issues, institutional needs, technological standards, installation, wiring, networking, licensing, and cost. The chief of the YSU-PD will make the final decision on new equipment installations and changes to equipment placement.

- (2) Cameras will only be permitted to be placed in public or restricted access areas and on university property. Cameras will not be placed in private areas or in a public area in order to view into private areas.
- (3) Any equipment currently in place as of the date of this policy will come under the control and authority of YSU-PD. YSU-PD will determine if the equipment currently in place meets ~~with~~ the institutional needs of the university and current technological standards for a CCTV recording system. YSU-PD will determine if any new equipment is permitted or if any current equipment is to be replaced or removed. No equipment is permitted unless recorded and controlled by YSU-PD or a specific exception is given by the YSU-PD. If an exception is given, the college or department is still required to comply with all other terms of this policy.
- (4) All equipment, where able, will utilize IP technology to transmit recordings, unless an exception is granted by YSU-PD. All legacy equipment currently in use at Youngstown state university will be converted to university standard technology within twelve months from the date of this ~~rule~~policy, unless an extension is granted by YSU-PD.
- (5) When an incident is reported or circumstances raise safety or security issues, the YSU-PD may authorize others to observe or review recordings or images.
- (6) In those areas that require on-site viewing or monitoring of CCTV equipment such as student residence halls, the director of the applicable office or department will designate an appropriate individual to serve as the contact with YSU-PD regarding the

equipment and will, at the beginning of the spring and fall semesters, provide a list to the YSU-PD of persons authorized to view or monitor the CCTV equipment. Viewing of these images shall be done only in restricted areas unless an exception is granted by the YSU-PD.

- (7) Each department or college with CCTV equipment will designate an appropriate individual within the department or college to serve as a contact with the YSU-PD regarding the equipment.
 - (8) Each department or college will be responsible for the cost of the equipment within the department or college.
 - (9) The chief of the YSU-PD shall be notified of any future university construction or any upgrading of existing university facilities prior to approval of the final designs of said facility if said facility is to include CCTV equipment. The chief of ~~police~~the YSU-PD or a designee appointed by the chief of ~~police~~the YSU-PD shall provide input into the placement of CCTV equipment during the design phase. The chief of the YSU-PD will make the final decision on new equipment installations.
 - (10) The chief of ~~police~~the YSU-PD shall be responsible for contracting any services for the ~~responsibility of~~ repair and service of all equipment.
 - (11) Any complaints involving violations of this policy shall be made to the university's office of general counsel and/or the chief of ~~police~~the YSU-PD.
- (E) Retention and release of information.
- (1) Retention of all recorded information is the responsibility of the YSU-PD except in the case of exceptions granted by the chief of ~~police~~the YSU-PD.
 - (2) It is the goal of the YSU-PD to retain recordings in a secure location and for thirty days; however, there are numerous factors that can limit retention, including but not limited to equipment capabilities. Specific image and/or audio files may be required to

be kept for a longer period at the direction of the office of general counsel and/or YSU-PD.

- (3) Recordings with information about a specific student are considered law enforcement records unless the university uses the recording for discipline purposes or makes the recording part of a student's education record.
- (4) Requests to view or to receive recording files from persons not authorized to access the system will be reviewed by the office of general counsel and the YSU-PD. The files will be distributed in an appropriately secured method. A log shall be maintained by the YSU-PD indicating the date and time range of the files, camera views, and the identification of the person receiving the files.
- (5) The recordings are considered security records under section 149.433 of the Revised Code because they are used to protect and maintain the security of the university. A record kept by a public office that is a security record is not a public record under section ~~149.433~~149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section. Any record requests, including subpoenas, will be directed to the office of general counsel for a response.
- (6) Any documentation, written or electronic, which identifies the location of all cameras installed on campus are considered security records under section 149.433 of the Revised Code, because they are used to protect and maintain the security of the university. A record kept by a public office that is a security record is not a public record under section ~~149.433~~149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section. Any record requests, including subpoenas, will be directed to the office of general counsel for a response.

Effective: 4/4/2019

CERTIFIED ELECTRONICALLY

Certification

03/25/2019

Date

Promulgated Under:	111.15
Statutory Authority:	3356
Rule Amplifies:	3356
Prior Effective Dates:	03/31/2015