USE OF SECURITY CAMERAS

SLT 6.29

Date of Last Update:
September 05, 2023

Approved By:

- Senior Leadership Team

Responsible Office:
Public Safety

POLICY STATEMENT

Grand Valley State University seeks to promote campus safety and to provide its community with a secure environment. Security video camera systems are a critical component to a comprehensive emergency and security plan. A security camera is defined as video technology that records a specific area in order to detect, deter, prevent, or investigate crime or other threats to public safety. The University takes seriously its responsibility to protect personal privacy when it operates security camera systems. No security camera will be installed on University owned or controlled property in any location for which there is a reasonable expectation of privacy. These areas include but are not limited to restrooms, locker rooms and occupied student residential rooms.

This policy applies to stationary security cameras owned or controlled by the University and not to portable or temporary camera applications. All other stationary cameras that are not for official University use, portable or not, are prohibited.

This policy serves to regulate the installation and appropriate uses of security cameras, including the retention, viewing, release and destruction of recorded images, data or records produced by security camera use.

The existence of this policy does not imply or guarantee that security video cameras will be monitored in real time, continuously or otherwise, nor that any particular department is going to observe and respond to a crime in progress.

Video recordings with information about a specific student are considered law enforcement records unless the University uses the recording for disciplinary purposes or makes the recording part of the educational record. The Department of Public Safety, working in

conjunction with the Information Technology Department has the authority to select, coordinate, operate, manage, and monitor all security camera systems pursuant to this policy.

PROCEDURES

Individual colleges, departments, programs, or organizations wishing to install security camera equipment for official University use on any of the University campuses are required to collaborate with Facilities Planning, Department of Public Safety and Information Technology prior to any installation. All equipment and installation must be approved and coordinated through the Department of Public Safety in order to meet the minimum technical specifications identified by the Department of Public Safety and Facilities Planning along with Information Technology for technical standards. All costs for purchase, installation, and maintenance of security cameras will be the responsibility of the appropriate project budget or the department/unit making the request. The University reserves the right to remove or disable cameras not compliant with this policy.

Security Camera System Operator

Security Camera System Operators are trained staff members who have access and been assigned responsibility by the Department of Public Safety. Prior to being permitted access to any security cameras, these individuals will be trained by the Department of Public Safety in the technical, legal, and ethical parameters of appropriate camera use. The Department of Public Safety will maintain an up-to-date list of authorized Security Camera System Operators having access to the system and any live or recorded images. Access to viewing, copying, duplicating and/or retransmission of live, recorded video or still images will be limited to Security Camera System Operators.

Security Camera System Operators are responsible to appropriately protect the privacy of personal information that may have been captured by cameras under their control.

Recordings

Images recorded by security camera systems are considered sensitive information that are to be protected from unauthorized access for modifications, duplications or destruction. The stored images generated by University security cameras are to be kept in a central location and secured in a network location established by the Information Technology department.

Stored data may be released when it is related to any criminal investigation, civil suit, subpoena or court order, arrest, or to aid in a disciplinary proceeding against a student or personnel actions against an employee. Stored data needing to be retained as part of a civil

or criminal investigation may be downloaded and retained by law enforcement personnel according to their individual department policies. Internal requests to release stored data are to be authorized by the Director of Public Safety or designee(s).

All recordings will be re-recorded over every 30 days unless there is a demonstrated business need, ongoing investigation, court order, or other bona fide use as approved by the Director of Public Safety or designee.

Monitoring

University security cameras are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: High risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the Director of Public Safety or designee(s).

Any person who tampers with or destroys video security equipment will be subject to criminal prosecution and/or campus disciplinary processes.