OP 91.315: ELECTRONIC SAFETY AND SECURITY

SCOPE

This policy applies to access control systems, video and electronic surveillance systems that monitor or record Mississippi State University facilities and/or faculty, staff, students and visitors using those facilities. The purpose of this policy is to provide uniform guidelines for the use of electronic safety and security systems on the campuses of Mississippi State University.

EXCLUSIONS

This policy does not apply to video used by or for:

a. Non-surveillance purposes. Examples of non-surveillance video recordings include, but are not limited to, video recordings made for:
   1. Instructional, academic, or artistic purposes
   2. Capturing public events and performances
   3. Recording promotional or news events
   4. Convenience such as weather or construction viewing
   5. Video conferencing
   6. University research purposes
   7. Patient care or medical treatment

b. The Mississippi State University Police Department (MSU PD). MSU PD is authorized to utilize video surveillance as necessary to fulfill their mission and responsibility as a law enforcement agency.

POLICY

It is the policy of Mississippi State University (MSU) to allow the use of electronic access control, surveillance cameras and security. Mississippi State University is committed to protecting the safety and property of our community by promoting a secure campus environment through the use of electronic safety and security systems in a professional and ethical manner in accordance with University policy and local, state and federal laws and regulations.

Virtual or “fake” surveillance cameras are prohibited.

Installation of “non-approved, non-university standard” systems is prohibited.

PROCEDURE

a. Approval and Installation:
   1. New or replacement electronic safety and security system equipment shall only be installed and operated following prior review and written approval by the Office of Life Safety and the Security, Video Management, and Access control committee.

2. Electronic Safety and Security System Project Request form will be submitted to request a review.

b. Inventory and Documentation:
    1. The Office of Life Safety shall maintain a master inventory and associated documentation of all existing and approved electronic safety and security systems, equipment and authorizations.

c. Management and Operation:
    1. Electronic safety and security systems installation, administration and management will be centralized and coordinated by the Office of Life Safety.
    2. The Office of Life Safety will operate the access control system and surveillance cameras or provide direct supervision of the use of such equipment by other departmental representatives.
    3. Evaluation of incidents with respect to camera placement will be completed annually by the Office of Life Safety.
    4. Maintenance and testing will be the responsibility of the Office of Life Safety.
    5. Departmental requests for system operators, using the Electronic Safety and Security Operator request form, will be submitted to the Security, Video Management, and Access control committee. Operators will be trained on the technical, legal and ethical use of video surveillance systems and perform their duties in accordance with this policy. All faculty, staff and students with access to electronic safety and security systems will receive a copy of this policy.

d. Camera Placement:
    1. Cameras may be used for monitoring publics areas and those areas where individuals would not have a reasonable expectation of privacy.
    2. Cameras shall not be approved for the following:
        i. Locker or dressing rooms
        ii. Restrooms
        iii. Individual offices, except with authorization to safeguard money, documents and supplies.
        iv. Areas for medical therapy or treatment
        v. Any other areas where individuals may have an expectation of privacy

e. Use of Cameras and Recordings:
    1. Monitoring individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other protected classification is prohibited.
    2. Surveillance cameras may not be used to monitor employee performance, work place attendance or work quality.

f. Storage and Retention:
    1. Surveillance images and access control logs will be stored in a secure data center to provide security controls and protection against unauthorized access, modification, duplication or destruction. Surveillance images and access control logs will be retained according to University policy and applicable state laws. Surveillance images and access control logs used in investigations will be retained longer than 90 days.

g. Release of footage:
    1. Footage will only be released in accordance with university policy.
    2. The Office of Life Safety will maintain close control over recorded images produced by surveillance cameras over which they have control.
    3. These images shall be available only to duly authorized officials of MSU operating within the course and scope of their official university duties.
    4. Materials will also be made available to authorized agencies or persons upon receipt by the Office of General Counsel of a duly issued subpoena.
    5. Any other release of footage will need approval of Security, Video Management, and Access control committee.
h. Key authority:
    1. The Security, Video Management, and Access control committee sets the standards and exercises authority regarding physical locks, access control of physical locks and locking standards.
    2. This committee will exercise authority and/or oversight over the issuing and revoking of key access on any university owned or controlled property.

EQUIPMENT TAMPERING

a. Tampering with electronic safety and security systems may result in a fine as established by the Security, Video Management, and Access control committee and/or disciplinary/employment action to the person(s) responsible. Tampering includes any activity that inhibits the functionality of video surveillance cameras or preventing access control doors from locking properly.

REVIEW

The Vice President for Student Affairs is responsible for the review of this operating policy every four years or as needed.

REVIEWED BY:

/s/ Regina Young Hyatt 02/07/2020
Vice President for Student Affairs

/s/ Timothy N. Chamblee 03/02/2020
Assistant Vice President and Director
Institutional Research and Effectiveness

/s/ Joan Lucas 03/03/2020
General Counsel

APPROVED:

/s/ Mark Keenum 03//06/2020
President