OP 91.315: ELECTRONIC SAFETY AND SECURITY

SCOPE

This policy applies to access control systems, video and electronic surveillance systems and license plate recognition cameras (LPR) 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 (HIPAA Compliance)

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.

DEFINITIONS

a. Integrated Security Management Division – a division of the Mississippi State University Police Department that is responsible for the security of people and MSU property through electronic security measures.

b. Electronic safety and security systems - This includes, but not limited to, locks (both electronic and manual), access control, license plate readers, intrusion alarms, and video surveillance cameras.
c. Security, Video Management and Access Control Committee – standing committee that sets university standards for locks, video security management systems, emergency lighting, access control and any other security protocols required to protect and enhance safety on any MSU owned property or facilities.
d. Office of Compliance and Risk Management (OCRM) – provides leadership and university wide collaboration that strengthens accountability, proactively and cooperatively manages significant risks, upholds a safe and healthy campus environment, and promotes and assists in compliance with state and federal laws.

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 Integrated Security Management Division of the Mississippi State University Police Department
    2. Electronic Safety and Security System Project Request form will be submitted to request a review.
b. Inventory and Documentation:
    1. The Integrated Security Management Division 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 Integrated Security Management Division.
    2. The Integrated Security Management Division 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 Integrated Security Management Division.
    4. Maintenance and testing will be the responsibility of the Integrated Security Management Division.
    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. License plate recognition (LPR) cameras:
    1. LPR cameras may be fixed or mobile
    2. LPR cameras may be used to enforce parking regulations
    3. "Hot lists" is a database of license plates of interest to law enforcement and parking enforcement. Hot lists may be used to identify the following:
        i. Stolen vehicles
        ii. Stolen license plates
        iii. Sex offender license plate information
        iv. Missing persons license plate information
        v. Gang or terrorist offender license plate information
        vi. Vehicle used in a crime license plate information
        vii. Locally wanted person(s) license plate information
        viii. Serious offender license plate information
        ix. Habitual DUI offender license plate information
        x. Person banned from MSU campus
        xi. Parking violations
f. 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.
g. 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.
h. Release of footage:
    1. Footage will only be released in accordance with university policy.
    2. The Integrated Security Management Division 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.
f. Training:
    1. Training of client users will be conducted by the Integrated Security Management Division (ISMD) staff when departmental staff are given access to the software.

g. Reporting of incidents:
    1. System operators monitoring or reviewing surveillance images are required to report any incidents, suspected incidents, or concerns directly to the appropriate department(s):
        i. Student-Related Incidents or Concerns: Report to the Dean of Students Office (e.g., disputes, concerns about student welfare).
        ii. Employee-Related Incidents or Concerns: Report to Human Resources (e.g., workplace injuries, concerns about employee behavior).
        iii. Emergencies, Criminal Activity, or Public Safety Concerns: Report to MSUPD (e.g., suspected thefts, vandalism, unauthorized access, concerns about security).
        iv. Bodily Injury, Property Damage, Unsafe or Risky Behaviors: Report to the Office of Compliance and Risk Management (OCRM) in addition to other appropriate departments, any incidents involving bodily injury, property damage, or unsafe or risky behaviors (e.g., slips and falls, damage to University property, damage to the property of others caused by University employees, anyone engaging in hazardous activities without proper safety measures)

i. 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

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 Hyatt 03/05/2024
Vice President for Student Affairs Date

/s/ Tracey N. Baham 03/19/2024
Associate Vice President, Institutional Strategy & Effectiveness Date

/s/ Joan Lucas 03/20/2024
General Counsel Date

APPROVED BY:

/s/ Mark E. Keenum 04/22/2024
President Date