THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

SECURITY CAMERA AND VIDEO SURVEILLANCE POLICY

Number 06.08.09

Division Finance and Administration – Office of Risk Management and Compliance

Date June 1, 2015 – Revised August 12, 2021

Purpose To establish a framework of rules and requirements that govern the installation and use of Security Cameras and related Security Camera Equipment on University property.

Policy

Scope: This Policy applies to all faculty, staff, students, and visitors while on the campus of The University of Alabama in Huntsville ("UAH" or "University") or at off campus locations controlled by the University.

Policy Statement: Security Cameras and associated Security Camera Equipment may only be installed on University property in a manner consistent with this Policy. This Policy supersedes any previous policy relating to Security Cameras and video surveillance.

Responsibilities and Authority: The Vice President for Finance and Administration ("VPFA") has delegated authority and responsibility to the Security Camera Administrator (as defined below) for:

- Developing and reviewing implementation strategies, standards, and procedures for security camera hardware and software application, operations, and maintenance;
- Authorizing the placement of security cameras and any related equipment;
- Maintaining the operational functionality of existing Security Cameras and associated Security Camera Equipment;
- Authorizing necessary purchases in accordance with University procurement procedures and policies;
- Undertaking supervisory, administrative, and other duties associated with the operation of the Security Camera System;
- Periodically auditing Educational/Research Camera Systems for compliance with this Policy; and

- Consulting and coordinating with the Chief of Police on matters relating to policy development, policy interpretations, and updates to this Policy.

The VPFA has delegated authority and responsibility to the Chief of Police for:

- Responding to internal and external requests for release of video recordings;
- Responding to and approving requests for access to the Security Camera System for viewing of live and/or recorded images;
- Approving audio recording through the Security Camera System;
- Reviewing contractor/vendor compliance with background check requirements of this Policy;
- Reviewing and providing input on Security Camera aspects of construction/renovation projects; and
- Consulting and coordinating with the Security Camera Administrator on matters relating to policy development, policy interpretations, and updates to this Policy.

Security Control Elements:

Training

All users of the Security Camera System will be instructed in the technical, legal, and ethical parameters of appropriate use. Each user must provide a written acknowledgment that they have read this Policy, understand the Policy contents, and agree to abide by the Policy before being granted access to the system.

Background Screening

All University employees and contractor/vendor employees involved in the installation, maintenance, and/or monitoring of Security Cameras must successfully pass a background screening including a criminal history check in accordance with the existing University background check policy prior to being approved access to or performing work on any part of the Security Camera System.

Contractors/vendors must certify to the University that their employees have successfully met the University's minimum requirements for background screening as outlined in this Policy and the University's background check policy, and must provide a copy of such background check(s) to the University's Chief of Police upon request.

Employees having regular access to recorded imagery – i.e., the ability to view and/or export recorded images – will be subject to background checks in accordance with the existing University background check policy. An employee's

home department/unit will be responsible for requesting and funding background checks required under this Policy. Notice of acceptable/unacceptable background check results relating to Security Camera access will be provided to the Chief of Police by the Human Resources department.

Placement Decision Making and Installation

The Security Camera Administrator shall be solely responsible for the technical oversight and functional operation of all Security Cameras on campus.

Colleges, departments, and other units desiring the installation and use of Security Cameras shall submit a request for such installation to the Security Camera Administrator. The Security Camera Administrator will consult with the Chief of Police or designee on camera placements where there is a public safety concern, criminal investigation, or where audio recording is requested, prior to approving requests.

The Security Camera Administrator shall work with stakeholders and/or the University Police Department as appropriate to determine the types of cameras and associated equipment needed to meet the intended application, and shall make recommendations on equipment specifications to ensure system interoperability and compliance with this Policy.

Installation of Security Cameras and other associated equipment shall be the financial responsibility of the requesting entity. Funding for maintenance and repairs of installed Security Cameras shall be the financial responsibility of the owning department/unit. The Security Camera Administrator is authorized to direct, oversee, and manage maintenance and repairs of all Security Camera System components.

Use of Security Cameras in Common Areas, as defined herein and including Common Areas inside student residence facilities, is authorized under this Policy.

Use of security cameras in sensitive and secure areas is permissible under this Policy. Sensitive and secure areas include mechanical spaces, areas other than residence facilities with controlled or secure access requirements and which are not accessible to the general public, server rooms, telecommunications closets, network infrastructure areas, data storage areas, records storage areas, areas where cash transactions occur, stockrooms, hazardous materials storage areas.

Use of Security Cameras inside Private Places, as defined herein, is prohibited.

Exterior mounted cameras shall not be purposefully aimed to view inside a Private Place, as defined below, or through a window of a privately-owned residence. If

needed, privacy masking will be utilized so a camera cannot inadvertently capture such images.

Use of mock or simulated security cameras are prohibited.

Audio recording through the Security Camera System requires the written approval of the Chief of Police and must be requested through the appropriate division's Vice President.

Any Security Camera Equipment not approved by the Security Camera Administrator is prohibited. Any equipment of this nature, when found, shall be removed immediately, and the responsible party may be subject to disciplinary action in accordance with applicable University policies and handbooks.

System Specifications and Design

Security Camera System hardware and software must meet the requirements of the most recent version of the University's *Security Camera System Specifications and Standards* document. Specifications and standards are modified periodically and may be obtained upon request from the Security Camera Administrator, who maintains the document.

Security Camera System designs for all new construction and renovation projects will be developed collaboratively by the Security Camera Administrator and the project Architect and/or Electrical/Security System Engineer in consultation with the Chief of Police or designee, Facilities and Operations, Office of Information Technology ("OIT"), and other key stakeholders (e.g., Housing and Residence Life will provide input into design of security camera systems intended for use inside residence halls).

All Security Cameras and associated Security Camera Equipment installed on University property shall be compatible with the University's central Video Management System ("VMS"). Security Cameras shall be supported by the VMS for camera-side motion detection, H.264 and/or H.265 video compression, password security, video recording (motion only, scheduled, and/or continuous), privacy masking, remote pan/tilt/zoom, remote focus/auto-focus, frame rate, video quality, and TCP/IP configuration. Equipment that cannot be configured through the VMS for all applicable settings listed above will not be compliant with this Policy.

The use of analog security cameras and associated equipment is restricted to existing legacy analog devices in service prior to January 1, 2020, and to specialized Security Cameras and equipment approved by the Security Camera Administrator and for which there is no cost-effective IP-capable equivalent.

Notification to the Public

The University will not generally provide notice that video recording systems in public areas are in use. Video with audio recording will typically be utilized in locations where the safety and security of minors is involved or financial transactions take place. For such areas, there shall be an approved notification placard or warning posted in plain view. Video with audio recording requires the written approval of the Chief of Police.

Use of Security Camera Recordings

Security Camera recordings are intended to be used for the purposes of enhancing public safety, deterring criminal activities, surveilling an area in real time, as an investigative tool to solve crimes and prosecute offenders after the crime has occurred, and as an investigative tool for accidents/injuries and other risk-related incidents.

The Security Camera System shall be utilized in a professional, ethical, and legal manner consistent with this Policy, other applicable University policies, and federal and state laws. Access to review live video feeds or recordings will be limited to those who have been properly authorized and vetted in accordance with the Policy.

Requests for regular, ongoing permissions to access recordings and/or obtain ongoing export permissions must be approved in writing by the Chief of Police or designee. Requests must originate from the employee's supervisory chain. Requests must include proof that the required background check, as outlined herein, has been completed and that the results of the check are acceptable. The Chief of Police or designee will review and approve requests based on a demonstrated and justified need for such regular, ongoing access. Employees with approved access may review and export video recordings as needed to perform their duties.

Other University employees acting in their official capacity and on an "as needed" basis, may be temporarily approved to review recordings. Approval must be granted by the Chief of Police or designee and the review process must be under controlled circumstances.

Security Camera recordings may be used for other purposes not inconsistent with the purposes of this Policy, including risk management purposes and sharing with outside law enforcement officials.

Users without permission to review recorded images are prohibited from capturing screen shots or otherwise capturing by any means any imagery provided through any component of the Security Camera System.

Release of Recorded Material

Requests for release of recorded material set forth in subpoenas, or other legal mechanisms compelling disclosure of said recordings, must first be submitted to the Office of Counsel, which will be responsible for reviewing the request with the appropriate University executives and administrators.

Approval of request for release of recorded material must be coordinated between the Office of Counsel, University administration, and the Chief of Police.

Release of recorded material beyond those described in this section shall be governed by applicable University policies and federal and state law.

Security Camera Monitoring

The existence of any signage or communication related to Security Camera use does not guarantee, nor is it intended to create a false sense of security by leading someone to believe, that Security Cameras are actively monitored in real time. The existence of this Policy does not imply or guarantee that security cameras will be actively monitored.

Monitoring may occur for purposes consistent with this Policy, including real-time observation; however, most often a review of recorded Security Camera recordings will be conducted after the fact.

Monitoring on the basis of a person's sex, race, gender, national origin, or other protected classification is strictly prohibited. Procedures must comply with all applicable University non-discrimination policies, as well as federal and state laws and regulations.

Retention of Security Camera Recordings

Recordings will typically be retained for thirty (30) days for common areas and for forty-five (45) days for areas where cash transactions regularly occur.

Retention times may be extended at the discretion of the University Police Department, Office of Counsel, Security Camera Administrator, or other appropriate University senior administrators, and as may be required by law, as part of a criminal investigation, court order, or risk-related incident investigation.

Protection and Retention of Security Camera Recordings

Video recordings shall be stored on servers accorded appropriate physical and electronic security with access by authorized personnel only.

All Security Cameras and associated equipment shall be connected to the central campus Security Camera System, and shall be compatible with the current VMS as indicated in this Policy.

Projects involving installation, removal, or modification of departmental/unit Security Cameras and associated Security Camera Equipment shall be reviewed and approved by the Security Camera Administrator prior to work being performed.

Departments requesting Security Cameras shall follow this Policy, including maintaining equipment records, employee training records, and ensuring equipment technological compliance with this Policy.

NDAA Section 889 Compliance:

All Security Camera Equipment shall be compliant with Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 ("NDAA"), and with any subsequent revisions or reauthorizations of the NDAA. The restrictions imposed under NDAA Section 889 shall further apply to Educational/Research Camera Systems and related components. Section 889 of the NDAA prohibits the use of specific security and telecommunications products and electronic components by recipients of federal funding, including federal contracts and grants funding.

Any Security Camera System or Educational/Research Camera System component not in compliance with the NDAA Section 889 requirements/prohibitions shall be removed from service at the expense of the owning department/unit.

Educational/Research Camera Systems:

Video cameras and video recording equipment considered to be Educational/Research Camera System equipment, as defined herein, may be used in an ancillary/secondary purpose as a Security Camera System with authorization from the Security Camera Administrator and the Chief of Police. Ancillary/secondary use of an Educational/Research Camera System for security purposes will make such system subject to all requirements under this Policy, including connection to the central Security Camera System and VMS. Such connection, including any necessary system modifications, will be at the expense of the owning department/unit.

Educational/Research Camera Systems that the Security Camera Administrator or the Chief of Police determine are being used for security purposes shall be reclassified as Security Cameras and Security Camera Equipment and shall be subject to all other requirements under this Policy, including connection to the central Security Camera System and VMS. Such connection, including any

necessary system modifications, shall be at the expense of the owning department/unit.

Educational/Research Camera Systems must be registered with the Security Camera Administrator. Educational/Research Camera Systems are subject to periodic audit by the Security Camera Administrator to ensure compliance with this Policy as it relates to security use and NDAA compliance.

Owning departments/units shall be solely responsible for maintenance and upkeep of Educational/Research Camera Systems.

Video Conferencing Cameras:

Video cameras and video recording equipment considered to be Video Conferencing Cameras, as defined herein, may not be used in an ancillary/secondary purpose as a Security Camera System. Ancillary/secondary use of a Video Conferencing Camera for security purposes will cause such system to be in direct violation of this Policy and subject to removal at the expense of the owning department/unit.

Miscellaneous:

Technical questions regarding the Security Camera System should be directed to the Security Camera Administrator.

Questions regarding access to recorded video, access to the VMS system for live viewing and approval for such requests should be directed to the Chief of Police.

The University's OIT shall not provide network access for Security Cameras or associated Security Camera Equipment unless the access request originates from the Security Camera Administrator.

Department/unit heads are responsible for ensuring compliance with all aspects of this Policy by users under their direct or indirect supervision.

Definitions:

Capitalized terms are defined as follows:

Common Areas: Areas which are not excluded under the definition of Private Places and which are available for use by more than one person or generally accessible to multiple facility occupants. Examples of common areas include, without limitation, lobbies, elevators, elevator landings, game rooms, study rooms, corridors and hallways including hallways leading to residential suites, stairwells, front attendant desks, reception areas, dining areas, kitchens, laundry rooms, storage areas, parking lots, sidewalks, greenways, landscaped areas,

playgrounds, courtyards, breezeways, conference rooms, meeting rooms, loading docks, classrooms (with approval of responsible Academic Affairs unit[s]), laboratories (with approval of responsible Academic Affairs and/or Research unit[s]).

Educational/Research Camera System: A video camera and/or related equipment used for image capture and recording for strictly educational and/or research purposes. Example educational/research uses include but are not limited to distance learning content delivery other than video conferencing use, lecture recording, testing services monitoring, and research documentation. Such camera systems shall not be considered Security Cameras as defined in this Policy so long as they do not have a direct or indirect (primary or ancillary) security use. Such systems are subject to periodic audit by the Security Camera Administrator. All such cameras shall comply with appropriate University policy and federal and state law, including but not limited to the NDAA, and, if applicable, HIPAA, FERPA, Institutional Review Board and other University policies.

Monitoring: The observation and operation of security cameras for the purposes of security surveillance. Monitoring may occur in real time or as an after-the-fact review of recorded images.

Video Conferencing Camera: A video camera, such as a USB-connected camera ("web cam"), handheld video camera ("camcorder"), video conferencing camera, and related equipment, when used exclusively for video conferencing purposes. Such equipment shall not be considered Security Cameras as defined in this Policy so long as they do not have a direct or indirect security use. Such system shall not be considered Educational/Research cameras so long as they are standalone units and not part of an Educational/Research Camera System. Video Conferencing Cameras shall not be subject to registration with or audit by the Security Camera Administrator unless or until such cameras are used in a manner inconsistent with this definition. All such cameras shall comply with appropriate University policy and federal and state law, including but not limited to the NDAA and, if applicable, relevant privacy laws.

Private Place: A place where one may reasonably expect to be safe from casual or hostile intrusion or surveillance, but not including a place to which the public or a substantial group of the public has access. Private places include, but are not limited to, residential rooms/suites, lactation rooms, patient treatment rooms, locker rooms, shower areas, and restrooms.

Security Camera: An approved video camera device used to capture, record, and/or transmit imagery to enhance public safety and property protection.

Security Camera Administrator: An individual appointed by the VPFA and delegated responsibility under this Policy for certain management and oversight functions relating to the Security Camera System. The VPFA may appoint, remove and replace the Security Camera Administrator at his or her sole discretion.

Security Camera Equipment: Services, software, or hardware other than video cameras used for control, operation, configuration, and administration of Security Cameras and the Security Camera System. This includes, but is not limited to, analog-to-digital encoders, network video recorders, digital video recorders, network equipment, viewing software, built-in or added audio capture devices, and recording software.

Security Camera System: The collection, in whole or in part, of Security Cameras and associated Security Camera Equipment under the control of the University, including such equipment at offsite locations.

University Property: Includes University owned, leased, or controlled property, both on and off campus, including buildings, offices, common spaces, labs, grounds, and other spaces.

Review: The University Police Department and the Security Camera Administrator are responsible for the review of this Policy every five (5) years, or sooner as circumstances require.