UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

UPGA - 15

VIDEO SURVEILLANCE POLICY

Number:	Name:	
UPGA-15	VIDEO SURVEILLANCE POLICY	
Purpose:		
The purpose of this policy is to provide the official Marshall University (MU) procedure to request, approve, design, install, operate, access, retain, and decommission MU video surveillance systems.		
Responsible Unit:		
Information Technology; Facilities & Operations/Planning & Construction; MU Police Department		
Approved by:		Approval Date:

1. General

    1.1 Scope:
    This policy applies to all University owned, University operated, University managed, or University supported video surveillance and electronic security camera systems, regardless of location or funding source, which are used for safety, security, law enforcement, compliance, or investigative. It governs the approval, installation, operation, access, retention, and decommissioning of such video surveillance systems across all University owned or University operated facilities.

    This policy does not govern routine recording conducted primarily for instructional, academic, research, clinical, operational, communications, or event documentation purposes (including lecture capture, research cameras, athletics video, event recordings, webcams, and video conferencing), except to the extent such recording is repurposed or configured for a surveillance purpose.

    Personal devices and third-party recording systems (including individually owned cameras and doorbells) are outside the scope of this policy; however, recording is prohibited in university designated locations where a reasonable expectation of

privacy exists (see Section 2.1.6), unless expressly authorized by the University and posted/consented as applicable.

Separate University policies and procedures (including conduct, housing, clinical, research, and records/retention policies) may apply to recordings and the spaces in which recordings occur. The University may accept personally recorded videos as evidence subject to MUPD intake procedures and legal review.

1.2 Authority:
Marshall University Chief Information Officer, as defined by ADMIN-20 Approval of Board of Governors Rules, University Policies and Administrative Procedures.

1.3 Controlling Over:
Marshall University owned and/or operated facilities.

2. Policy

2.1 General

2.1.1 Video Surveillance vs. Routine Recording

For purposes of this policy, video surveillance means the use of cameras or camera systems to monitor, observe, deter, or investigate behavior or incidents for safety, security, law enforcement, or compliance purposes, whether recorded or monitored live, and whether deployed in fixed locations or temporarily. In contrast, routine recording means recording or streaming conducted primarily for academic, instructional, research, clinical, operational, communications, or event documentation purposes where the intended use is not security monitoring or investigation (e.g., course capture, lab instrumentation, athletics performance review, or videoconferencing). The intended use of the recording, not merely the presence of a camera, determines whether this Video Surveillance Policy governs an activity.

2.1.2 Non-Surveillance / Exempted Uses

The following are not considered "video surveillance" when used for their primary non-security purpose, and are therefore outside the approval, access, and retention requirements of this policy (though other University policies and applicable law may apply):

- Instructional and academic recording (e.g., lecture capture, classroom recordings made as part of a course, recordings for accessibility accommodations, recordings for student presentations, and other course related documentation).
- Research and scholarly activity (e.g., cameras used for lab instrumentation, field research, observational studies, and other research data collection), subject to any applicable IRB requirements and research protocols.

- Athletics recordings (e.g., practice/game footage, performance analysis, and coaching review).
- Event recordings and communications (e.g., recordings of public events, performances, lectures open to the public, marketing/communications recordings, and University authorized media production).
- News media activity (e.g., TV news crews and other media operating pursuant to university approvals, space reservations, or applicable law).
- Webcams and videoconferencing (e.g., Zoom/Teams meetings, remote advising, telehealth/teletherapy when authorized, and other synchronous remote interaction tools) used for communication rather than security monitoring.
- Recordings for academic integrity and assessment (e.g., online exam proctoring and identity verification).

2.1.3 Legal and Regulatory Requirements

Video surveillance systems and related recordings must be implemented and used in compliance with applicable federal, state, and local law, Board of Governors rules, and University policy. Requirements that may apply include, but are not limited to:

- National Defense Authorization Act (NDAA), Section 889 and related federal supply chain restrictions on covered telecommunications and video surveillance equipment/services (to ensure University procured cameras and systems meet federal requirements).
- FERPA (Family Educational Rights and Privacy Act), where recordings may constitute student education records (including some classroom and proctoring recordings).
- West Virginia and other applicable state law governing privacy, recording, notice/consent, and interception of communications (particularly if audio is captured).
- Public records / open records requirements and related retention/production obligations, where applicable.
- CJIS and law enforcement evidence handling requirements, as applicable to MUPD investigations and chain of custody practices.
- HIPAA and other healthcare privacy obligations, where cameras are used in clinical spaces or capture protected health information.
- PCI DSS and other payment-card requirements, where cameras are used in cardholder data environments.

MUIT and STRG will maintain supporting procedures and standards that identify relevant requirements for video surveillance procurement, installation, and use, and will update those procedures as laws and regulations change.

2.1.4 Classrooms, Instructional Spaces, and Academic Freedom

Because classrooms and instructional spaces are central to academic freedom and open inquiry, video surveillance should not occur in classrooms and will not be installed or used for routine monitoring of classroom activity. Nothing in this policy prohibits ordinary course related recording (including lecture capture and recordings for accessibility) that is conducted for instructional purposes. Any proposal to use cameras in classrooms for a surveillance purpose must be reviewed and approved by STRG and General Counsel and must be narrowly tailored to a specific safety or security need.

Recordings created in connection with instruction or students (including online proctoring) may constitute education records and/or be subject to FERPA. Units making such recordings are responsible for ensuring appropriate notices, access controls, retention, and disclosure practices under applicable University policies and law.

2.1.5 Roles & Responsibilities

Marshall University Information Technology (MUIT), Marshall University Facilities and Operations and Planning and Construction (MUFO/P&C), Marshall University Environment Health & Safety (MU EHS), and Marshall University Police Department (MUPD) are collaboratively responsible for the equipment and software associated with the university's video surveillance system, as follows:

- MUIT: Provides the technical specifications for all security camera devices; manages the update and maintenance of the centralized and device-based video management software; provisions access to centralized and device-based video management software (in consultation with MUPD); maintains inventory and lifecycle of all security camera devices; audits functional operation and usage; trains users.
- MUFO/P&C: Designs/installs/maintains building infrastructure; ensures power, cabling, and mounting for video surveillance meet standards.
- MU EHS: Advises on privacy, signage, and life-safety considerations for video surveillance; supports risk assessments on video surveillance requests.
- MUPD: Coordinates investigations utilizing video surveillance; requests preservation holds to video surveillance; manages dispatch monitoring; collaborates on placement and incident response; approves access requests to centralized and device-based video management software.

2.1.6 Video Surveillance Protected Areas

Video surveillance devices will not be placed in locations where a reasonable expectation of privacy exists (e.g., restrooms, locker rooms,

treatment/ counseling rooms, student residential unit interiors), unless explicitly authorized by MUPD and/or General Counsel.

2.1.7 Video Surveillance Usage Restrictions

Video surveillance may be used only for legitimate University safety, security, and investigative purposes, consistent with this policy's definitions and approvals. Video surveillance may not be used for routine employee performance monitoring. Audio recording as part of video surveillance is prohibited unless specifically authorized by MUPD and/or University Counsel, except for student evaluation recording for academic purposes and other routine recordings that are outside the scope of this policy as described in Section 2.1.2.

2.1.8 Academic Freedom and Lawful Expressive Activity

Marshall University recognizes the importance of academic freedom and lawful expressive activity, including rights protected by the First Amendment where applicable. Video surveillance will not be deployed or used for the purpose of monitoring, recording, or deterring lawful speech, protest, assembly, academic inquiry, or other constitutionally protected expressive activity. Any use of video surveillance in connection with expressive activity must be based on a specific, documented safety or security need and must be narrowly tailored, time limited where feasible, and approved by STRG and University Counsel.

2.1.9 University Supported Video Surveillance Infrastructure

Marshall University Information Technology (MUIT), Marshall University Facilities and Operations (MUFO/P&C), Marshall University Environment Health & Safety (MU EHS), and Marshall University Police Department (MUPD) are collaboratively responsible for defining the video surveillance locations through all facilities owned and/or operated by Marshall University required for environmental safety. These locations will be considered the "university supported surveillance areas."

2.1.10 Requests for Additional Video Surveillance Infrastructure, Concerns, and Appeals

Any request for additional placements for video surveillance outside of the "university supported surveillance areas" must be approved by the Security Technology Review Group (STRG), comprised of delegates from each of the responsible units cited above. Requests for additional video surveillance must follow the following process:

1. Department/Unit will submit a Video Surveillance Technology Request including:
    a. Details related to the business need and risk/safety justification,
    b. Building map with proposed fields of view,
    c. Signage plan,
    d. Retention profile (default 10 days unless otherwise approved),

e. Funding source,
f. Impacted stakeholders.

2. STRG will review and either approve or deny video surveillance requests monthly for standards, privacy, and legal considerations. General Counsel will be engaged, as needed.
3. If approved, the requesting department/unit will be responsible for budgeting and funding the video surveillance device based on the standards set by MUIT. The requesting department/unit will also be responsible for budgeting and funding the replacement of the video surveillance device in accordance with end of support/end of life dates, security compliance requirements, or lifecycle replacement due to functional degradation. Outdated and/or unsupported equipment will be removed.

2.1.11 Appeal and Final Authority

A requesting individual or unit may appeal an STRG decision by submitting a written appeal within a reasonable time after the decision, stating the basis for the appeal and any added information. Appeals involving classrooms or instructional spaces will be decided by the provost (or designee) after consultation with STRG and University Counsel. Appeals involving other University spaces will be decided by the President (or designee) after consultation with STRG and University Counsel. The appeal decision is final.

2.1.12 Procurement of Video Surveillance Equipment

MUIT, in consultation with MUPD, selects devices that are available for procurement that meet the standards of video surveillance for the university. All equipment must be on the approved list and integrated with the enterprise VMS multi-campus solution. Standalone digital or network video recording systems are not permitted. Procurement of video surveillance equipment must align with MU purchasing rules. Personal or off-process purchases are prohibited.

2.1.13 Video Surveillance Installation

MUFO/P&Cs and MUIT are responsible for finalizing camera placement, setting up privacy zones (i.e., privacy masking), lighting, cabling, and segmented network controls (VLAN). MUIT is responsible for configuring firewall rules, device hardening, encryption, and NTP time synchronization. MUIT will enroll devices into video surveillance software, apply applicable naming conventions, set recording mode, and retention per policy. Any users of video surveillance software will be provided with role access with multi-factor authentication. Video surveillance signage will be installed and entrances/covered zones. All video surveillance devices will be tested by MUPD staff to verify field of view, image quality (including low light), recording, alerting, and time sync.

2.1.14 Video Surveillance Hardware Maintenance & Replacement

Marshall University Information Technology (MUIT), Marshall University Facilities and Operations/ Planning and Construction (MUFO/P&C), Marshall University Environment Health & Safety (MU EHS), and Marshall University Police Department (MUPD) are responsible for ensuring the operations of the "university supported video surveillance areas." Operations include quarterly inspection, testing, and maintenance on all systems. Video surveillance devices should be replaced in accordance with end of support/end of life dates, security compliance requirements, or lifecycle replacement due to functional degradation. Departments/units with video surveillance units outside of the "university supported video surveillance areas" are responsible for replacing their own respective devices, per university standards. If a department/unit chooses to decommission video surveillance devices, a request must be submitted to STRG. All video surveillance device media will be sanitized and destroyed, and signage will be removed.

2.1.15 Requests for Video Surveillance Content, Disclosure, & Evidence Handling

All requests for video surveillance content will be coordinated through MUPD. MUPD coordinates incident-related retrieval. Exports include case ID, timestamps, and watermark/hash, where feasible. MUPD will maintain a chain-of-custody log. The University General Counsel will manage and approve legal review, FOIA requests, and any external disclosures. All video surveillance exports are stored only on secured MU-managed locations. Personal USB drives or personal cloud storage are prohibited.

2.1.16 Requests for Video Surveillance Access

Continuous monitoring of video surveillance will be limited to authorized roles (e.g., MUPD dispatch) or time-bound approved needs. All system access is logged and auditable. Any users with video surveillance access must complete annual information security training including additional training in privacy and data protection. Video Surveillance Retention, Preservation, & Disposal.

2.1.17 Retention of Video Surveillance Content

The default retention period for video surveillance content is at least ten (10) days. A preservation hold may be placed for investigations/litigation with documented duration. Requests may be coordinated as defined in Section 2.1.15. Video surveillance will be automatically deleted when retention expires and no hold exists. Any media pending destruction must be protected until securely destroyed. Periodic audits will verify retention settings and deletion logs.

2.1.18 Compliance & Enforcement

Any unauthorized video surveillance systems will be disconnected, and violations of this policy may result in removal of equipment, access revocation, and employment/student discipline, per MU policy.