



SECURITY CAMERA & VIDEO FOOTAGE POLICY

4.5.26

1. Purpose	2
2. Scope	2
3. Definitions	2
4. Oversight	3
5. Approved Uses	3
6. Prohibited Uses	4
7. Camera Placement Standards.....	4
7.1 Permitted locations.....	5
7.2 Prohibited locations.....	5
8. Access to Live Feeds and Recorded Footage	5
8.1 Categories of authorized access	6
8.2 Training and acknowledgment.....	6
9. Footage Request Process	6
9.1 Preservation requests	6
9.2 Requests to review footage.....	7
9.3 Review and approval	7
9.4 Student, employee, and third-party requests.....	7
10. Release of Footage and External Requests	7
10.1 Internal release	8
10.2 External release.....	8
10.3 Law enforcement requests	8
10.4 Media release	8
11.Complaints, Misuse, and Violations.....	8
12. Exceptions.....	9
13. Review Cycle	9

1. Purpose

Milligan University uses security cameras to support the safety of students, employees, guests, and property; assist in emergency response; deter crime and misconduct; support legitimate investigations; and verify alarms, access-control events, and other safety-related incidents. This policy establishes how security camera footage may be collected, accessed, used, retained, released, and requested.

Security camera footage is the property of Milligan University and is considered sensitive institutional information. It will be handled in a secure, professional, ethical, and lawful manner. Access is not open by default. Footage may be viewed, exported, or released only for legitimate university business, safety, compliance, or investigative purposes and only by authorized personnel.

The existence of cameras does not mean footage is continuously monitored in real time, and it does not create a guarantee that all incidents will be observed, recorded, or retained.

2. Scope

This policy applies to all university-owned, university-managed, or university-networked security cameras and related video management systems located on property owned, leased, controlled, or operated by Milligan University.

This policy does **not** apply to:

- classroom, instructional, research, athletic coaching, marketing, livestream, or event-production cameras that are not primarily used for safety or security;
- personally owned devices or personal webcams;
- law enforcement body-worn cameras, or vehicle cameras.

If a camera system is used for security purposes, this policy applies regardless of which office purchased or requested it.

3. Definitions

Security camera system means cameras, recorders, servers, software, storage, and related infrastructure used to monitor or record video for safety or security purposes.

Recorded footage means any archived or exported video image captured by a security camera system.

Live view means real-time monitoring of a camera feed.

Authorized user means an employee who has been approved and trained to access live or recorded footage under this policy.

Personal or private areas means spaces where a person has a reasonable expectation of privacy, including but not limited to residence hall rooms, bathrooms, showers, locker or changing areas, medical or counseling treatment rooms, and similar spaces.

Preservation request means a request to prevent potentially relevant footage from being overwritten while a matter is reviewed.

4. Oversight

The Director of Campus Safety will have day-to-day operational authority over the university's security camera systems, including investigative review of footage, approval of access, maintenance of access logs, and coordination of footage preservation and release.

The Director of Campus Safety will:

- review and approve requests for new camera installations, relocations, major expansions, or decommissioning;
- oversee policy implementation, training expectations, retention practices, and access rules;
- review complaints, exceptions, and concerns regarding camera placement or use;
- recommend periodic updates to this policy and associated procedures; and
- conduct at least an annual review of the camera program and its compliance with this policy.

5. Approved Uses

Security camera systems may be used for the following purposes:

- protection of persons, facilities, and university property;

- daily monitoring entrances, exits, lobbies, parking lots, roadways, cash-handling points, access-controlled spaces, and other safety-sensitive locations;
- verification of alarms, access control events, or emergency conditions;
- review of reported criminal activity, safety incidents, property damage, theft, vandalism, trespassing, or other serious misconduct;
- support of university investigations involving student conduct, Title IX, Human Resources, risk management, or other official processes when the footage is relevant to the matter;
- support of law enforcement or emergency response when appropriate; and
- limited operational review necessary to maintain the integrity, functionality, or security of the camera system itself.

6. Prohibited Uses

Security camera systems and footage may **not** be used for:

- personal curiosity, entertainment, or any non-work-related reason;
- routine employee productivity monitoring or routine attendance monitoring, except where specifically authorized for a documented safety, regulatory, compliance, or investigative purpose;
- monitoring or targeting individuals based on race, color, national origin, sex, disability, religion, age, or any other protected characteristic;
- recording audio, unless separately approved in writing by the President or designee and legal counsel, and only where lawful;
- use of dummy, placebo, or misleading security cameras or signage; or
- use of facial recognition, biometric identification, or automated identity matching on security footage except where specifically approved in writing by the President or designee for an extraordinary safety threat, legal requirement, or criminal investigation and only if otherwise lawful.

7. Camera Placement Standards

7.1 Permitted locations

Cameras may be placed in public or common areas and in restricted-access areas where legitimate safety or security interests exist.

Examples include:

- building entrances and exits;

- parking lots and roadways;
- building perimeters and exterior gathering spaces;
- lobbies, vestibules, stairwells, and major corridors;
- residence hall entrances, lobbies, public lounges, and other approved common areas;
- labs, server rooms, mechanical rooms, storage areas, cashier points, and other sensitive or high-risk areas.

7.2 Prohibited locations

Unless required by law as part of a lawful criminal investigation, cameras may not be installed in:

- Inside residence hall rooms or apartments;
- bathrooms, shower rooms, or changing areas;
- locker rooms;
- counseling, health, or treatment rooms;
- single-occupancy offices where a heightened expectation of privacy exists; or
- any other area where a reasonable expectation of privacy exists.

Cameras may not be directed through the windows of private rooms, private residential spaces, or other locations where a person has a reasonable expectation of privacy.

8. Access to Live Feeds and Recorded Footage

Access to live or recorded footage will be limited to trained, authorized users with a legitimate need to know. Live monitoring is not required on a continuous basis and should be used selectively for emergencies, alarms, active incidents, special events, or specific safety concerns.

8.1 Categories of authorized access

Depending on the purpose of the request, access may be granted to:

- Campus Safety/Public Safety personnel;
- designated Information Technology personnel for technical maintenance;

- the Dean of Students or designee for student conduct matters;
- the Title IX Coordinator or designee for Title IX matters;
- the President, a Vice President, or their designee during emergencies or major incidents;
- legal counsel when needed for legal review, subpoena response, litigation hold, or risk management; and
- external law enforcement when appropriate for a criminal investigation or emergency response.

8.2 Training and acknowledgment

No employee may receive camera access until they:

- complete training on acceptable, ethical, legal, and technical use of the system;
- understand the limits of their authorization;
- acknowledge confidentiality obligations in writing; and
- are approved by the Campus Safety office.

9. Footage Request Process

9.1 Preservation requests

Any university office that becomes aware of an incident potentially captured on camera should promptly request preservation of the relevant footage. Preservation requests should be made as soon as practicable and, whenever possible, within **72 hours** of the incident so footage is not overwritten.

A preservation request should include, at minimum:

- requestor name and office;
- date of request;
- incident date and approximate time;
- location;
- brief description of the incident; and
- reason preservation is requested.

9.2 Requests to review footage

University employees seeking review of footage for an official purpose must submit a request to the Campus Safety office. Requests should include:

- the incident or business purpose;
- the relevant date, time range, and location;
- the specific reason footage is needed;
- the office requesting review; and
- whether the request is for viewing only, preservation, export, or formal release.

9.3 Review and approval

The Campus Safety office will review the request and determine whether:

- the request is sufficiently specific;
- the purpose is legitimate under this policy;
- the requester has a need to know;
- the request implicates student, employment, Title IX, litigation, or other protected processes requiring consultation; and
- legal counsel, Human Resources, Title IX, Student Development, Vice-President or another office must be consulted before access is granted.

9.4 Student, employee, and third-party requests

Students, employees, parents, and other third parties do not have a general right to directly view footage. In most cases, the university may review footage internally and provide a summary of findings or take appropriate action without allowing direct access to the recording itself.

10. Release of Footage and External Requests

Any exported copy of footage must be stored securely, tracked in an access/release log, and retained only as long as necessary for the purpose for which it was exported.

10.1 Internal release

Internal release of footage should be limited to the minimum necessary and only for approved official purposes.

10.2 External release

External requests for footage, including requests from attorneys, insurers, media, parents, or other third parties, must be routed through the Campus Safety office and reviewed by the President's office or legal counsel as appropriate.

Except where required by law, court order, subpoena, emergency circumstances, or other authorized university purpose, Milligan University will generally not release copies of security footage to outside parties.

10.3 Law enforcement requests

Law enforcement requests should be directed to the Campus Safety office. The university may share footage with law enforcement when appropriate for a criminal investigation, emergency response, or as otherwise required by law.

10.4 Media release

Release of footage or still images to the public or media for suspect identification, public safety messaging, or similar purposes requires approval from the President's office and consultation with legal counsel and university communications, as appropriate.

11.Complaints, Misuse, and Violations

Any complaint regarding camera placement, camera misuse, unauthorized viewing, improper disclosure, or other policy violations should be reported to the Campus Safety office.

Violations of this policy may result in:

- suspension or termination of camera access;
- employee discipline;
- student discipline, where applicable; and/or
- referral to law enforcement or legal authorities when warranted.

12. Exceptions

Exceptions to this policy must be approved in writing by the President or designee after consultation with the responsible Campus Safety/Public Safety office, Information Technology, and legal counsel as appropriate.

