Policy on Closed-Circuit Television (CCTV) Monitoring and Recording

I. Purpose

Rocky Mountain College is committed to maintaining a safe and secure environment for students, faculty, staff, and visitors. As part of a comprehensive security strategy, the College utilizes closed-circuit television (CCTV) technology to monitor and record activity in certain areas of campus.

The purpose of this policy is to establish guidelines governing the installation, operation, and use of CCTV systems on College property in a manner that enhances safety and security while respecting the reasonable expectations of privacy of members of the College community.

This policy applies to all students, faculty, staff, contractors, and visitors on Rocky Mountain College property or within College facilities.

II. General Principles

CCTV monitoring is intended to deter criminal activity, assist in maintaining a safe campus environment, and protect College property.

Permissible safety and security uses of CCTV include, but are not limited to:

- Protection of individuals, including students, faculty, staff, and visitors
- Protection of College-owned or operated property and facilities
- Monitoring building perimeters, entrances, exits, lobbies, corridors, receiving docks, laboratories, cashier locations, and special storage areas
- Verification of alarms and access control systems
- Monitoring common areas accessible to the public, including parking lots, transit stops, pedestrian walkways, and adjacent public streets
- Supporting investigations of criminal activity or serious violations of College policy, including acts such as theft, vandalism, or sabotage of research projects

CCTV technology shall not be used for purposes unrelated to campus safety or security.

All CCTV monitoring will be conducted in a professional, ethical, and lawful manner. Personnel responsible for monitoring or managing CCTV systems will receive appropriate training and supervision regarding the responsible use of this technology. Violations of this policy may result in disciplinary action consistent with College policies and employment regulations.

Information obtained through CCTV monitoring will only be released with the authorization of the Executive Vice President (EVP) or the Campus Safety Coordinator (CSC), except where disclosure is required by law.

Monitoring activities must comply with all applicable College policies, including the nondiscrimination policy, sexual harassment policy, and other relevant institutional policies. CCTV monitoring shall not target individuals based on protected characteristics such as race, gender, ethnicity, sexual orientation, national origin, disability, or other classifications protected by College policy or law.

CCTV systems will be used in a manner that respects reasonable expectations of privacy. Cameras will not be placed in locations where individuals have a heightened expectation of privacy, including but not limited to:

- Residential student rooms or suites
- Restrooms
- Locker rooms
- Changing areas

While cameras may be installed in certain residential hall common areas for security purposes, they will not be positioned in a manner that allows viewing into private living spaces.

The existence of CCTV cameras does not imply or guarantee that cameras are continuously monitored in real time.

III. Responsibilities and Authorization

The Campus Safety Department, in consultation with the Executive Vice President, is responsible for the oversight, implementation, and management of CCTV monitoring systems used for safety and security purposes.

All College departments utilizing CCTV systems must comply with this policy and associated procedures.

Authorization of CCTV Installations

The Executive Vice President is responsible for approving all permanent CCTV installations on campus.

The Campus Safety Coordinator may authorize temporary CCTV installations when necessary for:

- Criminal investigations

- Safety concerns
- Special events
- Other circumstances requiring enhanced security

Departments requesting installation of CCTV systems must submit a written request to the Executive Vice President or Campus Safety Coordinator. Requests must include:

1. A description of the safety or security concern justifying the installation
2. The number and proposed locations of cameras
3. The proposed monitoring method (e.g., real-time monitoring, alarm-triggered review, periodic review)

The Executive Vice President will make the final determination regarding the appropriateness of installation after weighing the security needs of the requesting department, the safety of the campus community, and the privacy interests of individuals who may be recorded.

Release of Recordings

Requests for CCTV recordings from external law enforcement agencies will be reviewed by the Campus Safety Coordinator and Executive Vice President in consultation with the College's General Counsel.

Requests for recordings related to internal College investigations or disciplinary matters will be submitted to the Executive Vice President, who will determine whether release is appropriate after considering privacy interests and the safety and security needs of the College.

Appeals

Appeals of decisions made by the Campus Safety Coordinator regarding CCTV use under this policy may be submitted to the Executive Vice President, whose decision will be final.

IV. Code of Procedures

The following procedures govern the operation and management of CCTV systems:

A. Compliance
All personnel involved in the operation or supervision of CCTV systems must comply with this policy and related procedures.

B. Camera Placement
The Campus Safety Coordinator will ensure that camera placement and fields of view comply with this policy, particularly with respect to residential facilities and private areas.

C. System Security
CCTV monitoring systems and control centers will be configured to prevent unauthorized access, tampering, duplication, or misuse of recorded data.

D. Retention of Recordings
CCTV recordings will normally be retained for approximately **45 days**, after which they will be automatically overwritten or deleted in the normal course of system operation.

Recordings may be retained for a longer period when necessary for:

- Criminal investigations
- Internal College investigations or disciplinary proceedings
- Litigation or anticipated litigation
- Compliance with legal obligations or law enforcement requests
- Other legitimate institutional purposes approved by the Executive Vice President or Campus Safety Coordinator

Any recordings retained for investigative or legal purposes will be maintained in a secure manner until the matter has been resolved.

E. Secure Storage
Recordings will be stored in secure systems accessible only to authorized personnel.

F. Supervised Access
Authorized personnel reviewing recordings must do so in accordance with established supervisory controls to ensure the integrity and appropriate use of recorded information.

G. Training
Personnel authorized to operate or access CCTV systems must receive training regarding the technical, legal, and ethical requirements governing their use. Operators will receive a copy of this policy and must acknowledge in writing that they have read and understand it.

H. Prohibition on Discriminatory Monitoring
Operators may not monitor individuals based on characteristics such as race, gender, ethnicity, sexual orientation, disability, or other protected classifications. Monitoring must be based solely on observed behavior or legitimate safety concerns.

I. Prohibited Viewing
Operators may not intentionally monitor private rooms or areas where individuals have a reasonable expectation of privacy.

J. Respect for Personal Privacy

Operators shall avoid prolonged or unnecessary observation of individuals engaged in lawful personal activity in public areas where no safety or security concern is present.

V. Notice and Signage

Rocky Mountain College recognizes the importance of transparency regarding the use of CCTV monitoring.

Signage will be posted in areas where CCTV monitoring is conducted to provide reasonable notice that video surveillance may occur. The signage will be placed in locations reasonably calculated to inform individuals entering monitored areas.

The purpose of such notice is to:

- Inform members of the campus community and visitors that security cameras are in use
- Promote deterrence of criminal activity
- Reinforce the College's commitment to responsible and transparent use of security technology

The absence of signage in a particular location does not necessarily indicate that CCTV monitoring is not occurring.

VI. Data Security and System Integrity

The College will implement reasonable administrative, technical, and physical safeguards to protect CCTV systems and recorded data from unauthorized access, misuse, or alteration.

These safeguards include, but are not limited to:

- Restricting system access to authorized personnel with legitimate operational responsibilities
- Password protection and secure authentication for system access
- Maintaining secure storage of recordings and system equipment
- Limiting the ability to copy, download, or distribute recorded footage
- Maintaining audit logs or other records of system access where technologically feasible

Unauthorized access, copying, disclosure, or distribution of CCTV recordings is strictly prohibited and may result in disciplinary action, up to and including termination of employment or referral to law enforcement.

VII. Review and Oversight

The CCTV program will be periodically reviewed to ensure compliance with this policy and to evaluate the effectiveness of CCTV monitoring in supporting campus safety.

The Campus Safety Coordinator, in consultation with the Executive Vice President, will conduct periodic reviews of:

- Camera placement and coverage areas
- Compliance with privacy protections
- Data retention practices
- System security and access controls
- Operational procedures for monitoring and review of recordings

Recommendations for improvements or modifications to the CCTV program may be made based on these reviews to ensure that the College continues to balance campus safety needs with the privacy rights of the College community.

VIII. Misuse of CCTV Systems

CCTV systems and recordings are the property of Rocky Mountain College and are intended solely for legitimate safety and security purposes.

Unauthorized use, access, copying, disclosure, alteration, or distribution of CCTV recordings is strictly prohibited.

Examples of misuse include, but are not limited to:

- Accessing recordings without a legitimate business purpose
- Sharing footage with unauthorized individuals
- Using CCTV systems to monitor individuals for personal reasons
- Posting or distributing recordings through social media or other external platforms without authorization

Violations of this policy may result in disciplinary action up to and including termination of employment, student disciplinary action, and/or referral to law enforcement where appropriate.

IX. Prohibition on Unauthorized Distribution of CCTV Footage

CCTV recordings are confidential security records of Rocky Mountain College.

Except as authorized under this policy or required by law, recordings obtained through the College's CCTV systems may not be copied, shared, distributed, published, or otherwise disclosed to any individual or organization outside the authorized review process.

Under no circumstances may CCTV recordings be:

- Posted or shared on social media platforms
- Provided to news media or other external parties
- Distributed electronically or through personal devices
- Used for entertainment, curiosity, or non-security purposes

Requests from the media or external parties for CCTV recordings must be referred to the Executive Vice President.

Any employee or student who improperly accesses, copies, or distributes CCTV recordings may be subject to disciplinary action up to and including termination of employment, student disciplinary action, and/or referral to law enforcement.

If you'd like, I can also show you **three optional provisions many colleges add that make this policy even stronger**, especially for accreditation and liability protection:

1. **FERPA protection language** (important because students appear in footage)
2. **Public records / media request handling**
3. **An administrative authority clause allowing relocation of cameras without rewriting policy**.

These additions are often the difference between a **good policy and a legally bulletproof one.**