VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 63) 15 July 2024

POLICY REGARDING SAFETY AND SECURITY CAMERA USE

1. **Policy:** This policy addresses the Institute's safety and security needs while respecting and preserving individual privacy. To ensure the protection of individual privacy rights in accordance with state and federal laws, this policy is adopted to formalize procedures for the installation of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records.

2. **Purpose:** The purpose of this policy is to regulate the use of Closed Circuit Television (CCTV) security camera systems used to observe and record public areas for the purposes of safety and security. The existence of this policy does not imply or guarantee that security cameras will be monitored in real time 24 hours a day, seven days a week.

3. **Responsibility:** The Deputy Superintendent of Finance and Support is responsible for (1) authorizing the selection, installation, coordination, operation, modification, management, and monitoring of all security cameras pursuant to this policy, except for covert security cameras authorized by the VMI Police, and (2) receiving complaints regarding the utilization and/or placement of security cameras and determining whether this policy is being followed. A form is included in this policy outlining the required information to request the installation of a security camera.

   Information Technology will review security camera requests to ensure compatibility with existing infrastructure.

   VMI Police and Information Technology shall be responsible for: (1) the implementation of this policy and for reviewing requests for security camera installations and, (2) monitoring developments in the law, security industry practices, and technology to ensure that installed security cameras are consistent with best practices and comply with federal and state laws.

   Ownership of the CCTV security camera systems belongs to the VMI Police. VMI Police are responsible to: (1) review and recommend to the Deputy Superintendent of Finance, Adminstation, and Support the specific placement of security cameras after determining conformance to this policy, (2) test and verify the security cameras and supporting systems are working, and (3) notify the Physical Plant of needed repairs.

   Physical Plant shall be responsible for installation and routine maintenance of security camera systems.

   The Executive Assistant to the Superintendent will review all external public and media requests for release of records and footage obtained through security cameras and present all requests to the Deputy Superintendent of Finance, Administration, and Support.

Information obtained through security camera video recording will be used for security and law enforcement purposes. The copying, duplicating, and/or retransmission of recorded video shall only be authorized by one of the following:

- Superintendent
- Deputy Superintendent of Finance, Administration, and Support
- VMI Chief of Police

4. **Scope:** This policy applies to all personnel and departments of VMI in the use of security cameras and their monitoring and recording systems. Security cameras may be installed in situations and locations where the security and safety of either property or persons would be enhanced. Security cameras will be limited to uses that do not violate a reasonable expectation of privacy. Where appropriate, security cameras may be placed Post-wide, inside and outside of buildings. Audio recording from security cameras is prohibited.

   Legitimate safety and security purposes for a security camera monitoring system include:

   A. Property Protection: To deter thefts and acts of vandalism or to capture such incidents if they do occur.

   B. Personal Safety: To deter crimes against persons or to capture incidents if they do occur. This includes the use for prevention of and response to sexual misconduct as outlined in General Order #16, Discrimination, Harrassment, and Sexual Misconduct Policy.

   C. Extended Responsibility: To monitor areas from a remote location when necessary due to lack of personnel or to enhance the security of the area being monitored.

5. **Placement of Cameras:** The locations where security cameras are installed may be restricted access sites such as a departmental computer lab; however, these locations are not places where a person has a reasonable expectation of privacy. Security cameras will be located so that personal privacy is maximized. Unless being used for criminal investigations, the location of security cameras will be visible.

   Security camera positions that include views of faculty/staff residential housing shall be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy. Security cameras in Barracks may view arches, entry/exit points, hallways/stoops, and courtyards.

   Unless the security camera is being used for criminal investigations by the VMI Police or other law enforcement agency, monitoring by security cameras in the following locations is prohibited:

   - Restrooms
   - Locker rooms
   - Offices
   - Classrooms

   The installation of “dummy” security cameras is prohibited.

6. **Access and Monitoring:** All recording or monitoring of activities of individuals or groups by Institute security cameras will be conducted in a manner consistent with VMI policies and state and federal laws, and will not be based on the subjects' personal characteristics or status, including race, sex, color, national origin, religion, age, veteran status, sexual orientation, pregnancy, genetic information, disability, or other protected characteristics. Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner.

   All personnel with access to view live video from Institute security cameras must be trained by the VMI Police in the technical, legal, and ethical parameters of monitoring equipment. A copy of this policy and related standards of appropriate use will be provided to users. Upon separation from the Institute, access privileges to the CCTV systems will be withdrawn within 24 hours.

   Institute security cameras are not monitored continuously under normal operating conditions, but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: high risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the VMI Chief of Police or his/her designee.

   The Superintendent, Deputy Superintendent of Finance, Administration, and Support, or VMI Chief of Police may grant authorization for users to be trained to monitor live video from the CCTV systems. Access to monitor live video from security cameras shall be limited to authorized personnel and only for purposes related to the performance of duties pertaining to that authorization. This policy provides authorization to monitor live video from a security camera to (1) all VMI Police Officers, (2) employees of the VMI Museum System, (3) members of the Commandant Staff including the Officers in Charge, Assistant Officers in Charge, (4) Director of Emergency Management, and (5) the Inspector General and Title IX Officer.

   Access to recorded and stored video from cameras shall be limited to the VMI Police for official use of law enforcement. Other requests for recorded video footage will be made through the Deputy Superintendent of Finance, Administration and Support to the Superintendent. Any disclosure of recorded and stored video will be in accordance with the Family Educational Rights and Privacy Act (FERPA), as applicable.

   Cadets are not authorized to monitor or access live or recorded video of the CCTV systems unless the cadets are (1) in an official capacity as part of the guard team where authorization is granted to view only live video of entrances and exits of the Barracks, or (2) in an official capacity and have received written approval from the Superintendent to access either live or recorded video.

   Unathorized access to the CCTV systems is not allowed and will not be tolerated. If the system is accessed by an unauthorized person, the VMI Police will be notified and will investigate the allegations of unauthorized access. Unauthorized access of the CCTV systems or intentional destruction of or tampering with cameras or monitoring equipment by cadets or employees will result, in most cases, in administrative discipline and sanctions up to and including dismissal or termination.

7. **Appropriate Use and Confidentiality:** Information obtained from security cameras shall be used for safety and security purposes and for law and policy enforcement, including, where appropriate, Cadet functions (Honor Court, General Committee, Executive Committee, Officer of the Guard Association, etc.). Requests for cadet organizations to access live or recorded video will be submitted by the appropriate Officer in Charge of the specific cadet organization to the Deputy Superintendent of Finance, Administration, and Support. Information must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure in accordance with General Order # 21, Records Management Policy, and FERPA.

   All appropriate measures must be taken to protect an individual's right to privacy and hold Institute information securely through its creation, storage, transmission, use, and deletion.

   All security camera installations are subject to any applicable federal and state laws.

   Personnel are prohibited from using or disseminating information acquired from Institute security cameras, except for official purposes. All information and/or observations made in the use of security cameras are considered confidential and can only be used for official Institute and law enforcement purposes.

8. **Use of Cameras for Criminal Investigations:** Mobile or hidden video equipment may be used in criminal investigations by the VMI Police Department. Covert video equipment also may be used for non-criminal investigations of specific instances which may be a significant risk to public safety, security, and property as authorized by the VMI Chief of Police or his/her designee.

9. **Exceptions:** This policy does not apply to:

   A. Cameras used for academic purposes. Cameras that are used for research are governed by other policies involving human subjects and are, therefore, excluded from this policy.

   B. Webcams for general use by the Institute (e.g., on the official VMI website).

   C. Video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Examples of such excluded activities would include videotaping of athletic events for post-game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons.

   D. Audio/video recording equipment in VMI Police vehicles or department issued body cameras worn by VMI Police Officers.

   E. Video that is streamed to or posted to the internet for public affairs projects approved by the Director of Communications and Marketing.

   F. Automated teller machines (ATMs), which utilize security cameras.

10. **Storage and Retention of Recordings:** No attempt shall be made to alter any part of any security camera recording. Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.

All security camera recordings shall be stored for a period of no less than 60 days, after which they may be erased or written over, unless retained as part of a criminal investigation or court proceedings (criminal or civil), in reasonable anticipation of litigation, for administrative or internal investigation, or other bona fide use as approved by the VMI Chief of Police or VMI legal counsel. Individual departments shall not store security camera recordings.

A log shall be maintained by VMI Police of all instances of access to or use of security camera records. The log shall include the date and identification of the person or persons to whom access was granted.

FOR THE SUPERINTENDENT:

John M. Young
Colonel, Virginia Militia
Chief of Staff

DIST: E, Cadets

OPR: Ops & Planning/VMI Police

REQUEST FOR SECURITY CAMERA INSTALLATION

In accordance with General Order 63, request is hereby made to install a security camera or modify an existing security camera as outlined below.

Requestor	Department	Date
Facility/Building/Area Location:		
Describe Purpose of Installation/Modification:		
Describe Security Camera Locations and Monitoring Locations:		
Describe Requirements for Live Feed or Recording:		
Names of Personnel to Have Access to Security Camera System:		
PHYSICAL PLANT – Project Information		
Estimated Installation Cost		$
Estimated Annual Maintenance Cost		$
INFORMATION TECHNOLOGY – Request Meets IT Requirements		
Signature Approval:		Date:
VMI POLICE – Request Meets Police Requirements		
Signature Approval:		Date:
ASSISTANT SUPERINTENDENTOF OPERATIONS AND PLANNING APPROVAL		
Signature Approval:		Date:

Virginia Military Institute

Police Department

Security Camera Use Policy Training Log

Employee	Date Policy Received	Date of Review	Employee Signature	Policy