SECURITY CAMERA SYSTEMS POLICY
PROCEDURES AND GUIDELINES

These procedures support the Security Camera Systems Policy by outlining the implementation requirements for installation, access, data storage, and management of surveillance equipment at CSU.

1. RESPONSIBILITIES OF UNITS
    - All proposed VMS (Video Management System) Device installations must be submitted to and approved by the Campus Security Systems (CSS) Department.
    - Units bear financial responsibility for all equipment, maintenance, licensing, and repairs for equipment installed.
        - The responsibility of the CSS Department is for installation, licensing, maintenance, and repairs of VMS equipment installed for primary building ingress/egress, university common areas, cash handling areas, and highly restricted areas; as determined by CSS in consultation with Safety & Risk Services per industry standards.
        - Any installation, maintenance or repairs must be coordinated through the CSS Department.
    - Units must designate and request authorized users for VMS access.
2. INSTALLATION PROCEDURES
    - Permanent Installations
        - Must be reviewed and approved by the CSS Department.
        - Equipment must be compatible with the VMS system, unless otherwise approved by the CSS Department and in compliance with the Procurement Rules.
    - Temporary Installations
        - Must be reviewed and approved by the CSS Department.
        - Limited to 60 days unless otherwise authorized.
        - Construction cameras independent of the university VMS system, temporarily set up by General Contractors for security of the jobsite are not subject to these procedures.

- Modifications to Existing Installations
    - Must be reviewed and approved by the CSS Department before any changes are made.
    - CSS may audit installations for policy compliance and recommend changes.
- Any installation of a VMS Device must follow CSU Construction Standards.

3. STORAGE, RETENTION, AND ACCESS
    - All VMS Data must be stored digitally on a secure CSS-managed server.
    - Retention is a minimum of 20 days, with extensions for legal or regulatory compliance.
    - Access to stored Data is determined by an individual's approved level of access to the camera system ("Archive" Access vs "live" access)
    - If access to stored data is required beyond the minimum retention period, a Stored Data Request must be electronically submitted and approved by the CSS Department.
        - Any data exported from the system to be saved and accessed beyond the minimum retention period will be subject to university retention policies.
4. VMS DATA EXPORT
    - Export of VMS data is not allowed unless legally required.
        - Compliance with subpoenas must be coordinated with the Office of General Counsel.
5. AUDIO AND PRIVACY-SENSITIVE SURVEILLANCE
    - Audio Surveillance requires compelling justification.
    - The duration of audio recordings should be minimized except in limited circumstances where there is a legitimate business or security need, such as student disciplinary proceedings, applicable service desks or other areas as approved by CSS.
    - Notification is required unless it jeopardizes safety or investigation.
    - Surveillance must avoid capturing academic or research activity when possible.
6. RESIDENTIAL FACILITIES CONSIDERATIONS
    - Surveillance must be limited to exteriors and common areas unless authorized for investigation.

7. SECURITY OF EQUIPMENT
    - Cameras and equipment must be tamper-proof and fiber connections to the servers must be secured in locked, controlled spaces (i.e., data closets).
    - When possible, cabling should be housed in EMT conduit.
8. VMS USER TRAINING
    - Any access request must be reviewed and approved by the CSS Department.
    - The online training must be completed.
    - All VMS users must review the Policy and Procedures and sign acknowledgment of compliance.
    - Background checks are required: every 5 years for Archive/Live access; waived for police personnel with access to the camera system, due to the extensive background check related to their position.
    - CSS will provide or facilitate training for all VMS Client Operators beyond online training if necessary.

These procedures ensure consistent application of surveillance systems in alignment with CSU values of privacy, safety, and operational integrity.