# Planning Notes
# AP 6510 – Networked Video Cameras

## DEFINITION:

A networked video camera is a camera placed or installed for long term use that is remotely viewable via a coax or network connection. This AP is not intended to address the use of portable video equipment on campus, those uses are addressed in AP 3710 (pending Board review in November 2016)

## CLASSES OF CAMERA INSTALLATIONS:

### 1. Instructional Support

- Cameras must be used in direct support of instructional activities.
- Cameras in this class are not **typically** used for security purposes (see below)
- Installation requests approved by Dean of the area, reviewed by VP of Instruction.
- Control and viewing authority established by Department.
- Unless required for instructional purposes, the output of an instructional camera may not be recorded or archived. Exceptions to this policy are granted by the approving VP.
- Unless required for instructional purposes, video analytic software may not be used on the output of these cameras. Exceptions to this policy are granted by the approving VP.
- Current examples include cameras installed in Vet Tech surgery room, cameras installed over instructor's drafting table in drafting classrooms, cameras installed in demonstration kitchens, cameras installed in Child Development Center, cameras used in television production facilities, cameras used for lecture capture in Professional Development and cameras used to proctor testing facilities.

### 2. Operational Support

- Cameras must be used for non-instructional operational support activities. Use of these cameras is required to enhance the operational aspects of a facility.
- Cameras in this class are not **typically** used for security purposes (see below)
- Installation requests are approved by the appropriate VP and reviewed by cabinet.
- Control and viewing authority established by approving VP.
- The output of these cameras may not be recorded or archived. Analytic software may not be applied to the output of these cameras.
- Current examples include cameras in the audience area of the Performing Arts Center, Construction Cameras, door cameras used to admit individuals, cameras in the Founders Hall Board Room, cameras in the Emergency Operations Center.

- Installed cameras used exclusively for video conferencing are included in this class.

3. **Asset Protection**

    - Cameras used to protect physical assets on the campus. These cameras are only intended to protect physical assets and their presence must be marked with clear, approved signage.
    - Cameras in this class are not **typically** used for security purposes (see below)
    - Installation requests are approved by Campus Safety, and are reviewed by the VP of Administrative Services and cabinet. Camera systems installed on campus property by outside providers, such as Sodexo, must follow this procedure.
    - Control and viewing authority established by the VP of Administrative Services. These cameras are not typically monitored in real time, as a result, no emergency response should be anticipated in the event of a security related incident.
    - The output of these cameras will be recorded and archived for subsequent action in the event of an asset loss. Retention policies are established by Cabinet.
    - Analytic software such as motion detection and object analysis may be applied to the output of these cameras.
    - Current examples include cameras in vault areas, loss prevention cameras in the SAC Book Rac, cameras in the Prime Stop, cameras in the warehouse, the camera in the music locker area of Building 2M, cameras in Chemistry stockrooms and in the Cadaver Lab, both located in Building 60.

4. **Security**

    - Cameras intended to enhance the personal security of individuals on campus. The presence of these cameras must be marked with clear, approve signage.
    - Installation requests are approved by Campus Safety, and are reviewed by the VP of Administrative Services and cabinet.
    - Control and viewing authority established by the VP of Administrative Services. These cameras may be monitored in real time in order to provide the appropriate security response.
    - The output of these cameras will be recorded and archived for subsequent action in the event of an incident. Retention policies are established by Cabinet.
    - Analytic software such as motion detection and object analysis may be applied to the output of these cameras.
    - Current examples include cameras placed in public interior and exterior areas in Building 9B, and the camera at the door between the emergency exit of the Print Shop and the HR offices.

## DESIGN PHILOSOPHY as recommended by ASCIP

All classes of cameras should be accessible by a common Video Management System (VMS) to simplify maintenance and support. In the event of an emergency, all camera assets should be accessible by campus police in order to provide essential logistical information for emergency response. Additionally, the VMS must support access logs to insure compliance with privacy controls established by the procedure.

The District should employ a philosophy of perimeter coverage for security cameras. Security cameras should be deployed and focused on the perimeter of buildings and the campus as a whole.

Except for instructional or operational support usage, cameras may not be placed inside a classroom, laboratory, library or any other area used as a classroom or study space. Cameras may never be placed in areas such as restrooms, locker rooms, private offices or staff lounges where there is a reasonable expectation of privacy by students or staff unless the installation is associated with an ongoing investigation by an authorized law enforcement agency.

Cameras used for asset protection should be clearly labeled with language such as "*To reduce property damage to our facilities, this campus has installed video surveillance cameras*". Signage should be of an appropriate size and placed such that a reasonable person would be able to discern the contents of the sign.

Authorized users as approved through the process detailed above shall receive training on the use of the VMS, to include rules relating to District policies and procedures. Users shall receive training on the technical use of the system and how to use controls to maximize efficiency and clarity of image. Authorized users are subject to audit on the use of the system and must restrict the use of the system to the intended purposes.

Except for designated instructional uses, information stored on the VMS shall be used exclusively for security and law enforcement purposes. The use of information on the VMS for use in gathering evidence for use in internal employment of labor related investigations is strictly prohibited. Except for designated instructional purposes, sound may not be recorded or monitored by the VMS.

Camera systems may not be modified, moved or relocated without approval from the appropriate Vice President and review by Cabinet. New installations must be coordinated by the Technical Services Division in cooperation with the Information Technology Division in order to insure compliance with District Standards and to protect the integrity of the campus network.

Policies for the storage and recall of archived information on the VMS shall be established prior to the deployment of any new campus systems. The VMS system shall be configured to provide forensic authentication of the stored material when required for legal action.

The integrity of the entire video system should be routinely audited to insure compliance with established policy.

Policies regarding the placement and use of video cameras must be bargained with employee groups regarding the effects of camera usage on employee discipline and evaluations.