2.1400 Video Monitoring & Recording

A. The Department of Public Safety's Building Security Systems Unit coordinates, installs, and maintains the university's video monitoring and recording system.

B. The video system:
   1. Is monitored in the Security Operations Center using secure servers;
   2. Allows cameras to be set to record continuously or activated by motion;
   3. Retains images for at least 14 days before being automatically overwritten.

C. The agency has certain video monitoring and recording responsibilities that include, but are not limited to:
   1. A documented yearly review conducted which reviews incidents that involved video monitoring and the effectiveness of camera locations;
   2. Making recommendations for camera locations based on the University's needs and in consultation with construction authorities and stakeholders for the locations of proposed cameras; and
   3. Monitoring and using the system to:
      a. Enhance public safety;
      b. Prevent and deter crime and public disorder;
      c. Identify criminal suspects and activities;
      d. Gather evidence;
      e. Document police actions to safeguard citizen and officer rights;
      f. Assist in the deployment of police assets.

D. The Security Operations Center is designated as a limited access area consistent with 1.412 Security of Agency Facilities & Equipment.
   1. Bureau commanders, employees assigned to the Security Operations Center Unit, Criminal Investigations Unit, and designated Building Security Systems personnel are granted unlimited access to the Security Operations Center.
   2. Other personnel are permitted to be in the Security Operations Center only when:
      a. In the furtherance of agency business or active ties, they are admitted and escorted by agency employees with un-limited access;
      b. *Bona fide* emergencies exist.

E. Various employees have differing levels of video system access and permissions as follows:
   1. Security Operations Center Security Monitors have the ability to control cameras on the system and have access to live video.
   2. Only the Security Operations Center (SOC) supervisors, administrators, designated personnel and certain Building Security technicians have access to recorded video on the system;
   3. SOC Supervisors have user rights with the ability to take control of cameras being operated by other SOC Employees;
   4. Police Communications Operators and police officers have the ability to view live video in the temporary holding facility.

F. Building Security Systems personnel are responsible for the maintenance and testing of the system.
   1. All users should report video system maintenance and operational problems through the Building Security Systems on-line work order system.

G. Video system use:
   1. Must be conducted only for *bona fide* agency business;
   2. All personnel involved in the supervision, application, use or monitoring of CCTV installations, collection of video or digital data, or other aspects of CCTV use, must receive appropriate training including, but not limited to the ethical limits of CCTV use.
   3. Will be consistent with operating instructions in the Security Operations Center and related on-the job training conducted during employees' field training or orientation programs as applicable to their job duties;
   4. Is conducted mainly as random and directed video patrols by SOC Employees;
   5. Is permitted as an immediate, incident driven observation resource or follow-up investigative tool;
   6. Is not allowed to target persons for monitoring based on any illegal or improper criteria;
   7. May take into account the race, ethnicity, gender, or other demographic criteria based on trustworthy, locally relevant information that links persons of certain description criteria to particular unlawful or suspicious activities consistent with 2.431 Impartial Policing;
   8. May take into account public safety concerns and monitor persons engaged in First Amendment activities so long as the monitoring conforms to 2.362.10 Criminal Intelligence Procedural Safeguards.

H. Retrieval of Recorded Video
   1. Video Requests—Law Enforcement
      a. In order for UMDPS to conduct a Video Review, a law enforcement officer with jurisdiction over an incident that has been reported must submit a "Video Review Request" using the on-line video review request system.
      b. In the event a Video Review conducted by UMDPS yields information believed to be related to the subject of a Video Review Request, UMDPS will burn the applicable video images to appropriate electronic media.
      c. The video images that are burned will be submitted to the UMDPS Logistics Unit where the images will be maintained as evidence.
      d. A copy of the media submitted to UMDPS Logistics will be made available to the officer making the original Video Review Request
      e. A copy of the written Video Review Report will be provided to the officer making the original request as appropriate.
      f. Video recordings are stored for approximately 14 days after the incident. Some recording devices may retain the data for longer periods depending on the size of the server. For this reason, requests for video reviews should be sub-

mitted as soon as possible. Videos with evidentiary value will be submitted to Logistics for proper handling and storage.

2. Video Requests—Third Parties
   a. UMDPS will provide copies of raw video recorded on the CCTV System for specified dates, times and locations when required by court issued subpoenas or Maryland Public Information Act (PIA) requests.
   b. In the event a subpoena or Maryland Public Information Act (PIA) request is received, a copy of the information should be provided to the UMDPS Subpoena Coordinator and the SOC Commander as soon as practical via electronic mail.
   c. Maryland Public Information Act (PIA) requests must be in writing and should contain detailed information, including the date, time, and precise location of the incident for which video is requested.
   d. Individuals wishing to request video pursuant to a PIA request should visit the following website: http://www.umd.edu/pia/index.cfm.
   e. The individual submitting a subpoena or making a PIA request will be informed as to where and when the disks may be retrieved and the total cost for the work performed.