FLORIDA ATLANTIC UNIVERSITY

Office of the President
University Policy

SUBJECT:	**Effective Date:**	**Policy Number:**	
VIDEO SURVEILLANCE	5-31-11	1.11	
	Supersedes:	**Page**	**Of**
	New	**1**	**7**
	Responsible Authority:		
	Chief of Police		

APPLICABILITY:

This policy is applicable to all members of the University community, including all students, faculty, staff and all visitors, contractors and guests to the University or any of its campuses, facilities or events.

POLICY STATEMENT:

I. Introduction. Florida Atlantic University is committed to the enhancement of public safety, the quality of life, and providing an environment conducive to quality education, individual privacy, diversity, and freedom of expression. Accordingly, the University has elected to utilize closed-circuit television (CCTV) to monitor public areas in order to deter crime and assist the University Police Department (FAUPD) in maximizing the security and safety of individuals and property that are part of the University community. Any diversion of security technologies for purposes other than those listed in this policy would undermine the acceptability of these resources for critical safety goals and is therefore strictly prohibited.

II. Purpose. The purpose of this policy is to provide guidelines for the use of CCTV on University property and facilities in a way that enhances security, while at the same time respects privacy. Further, this policy is intended to formalize procedures for the installation, monitoring, storing, dissemination and destruction of surveillance records. *The existence of this policy does not imply or guarantee that cameras will be monitored in real time twenty-four (24) hours a day, seven (7) days a week.*

III. Definitions. The following definitions apply to terms as used in this policy:

a. *CCTV*: Closed circuit television that can be used to remotely monitor and record activity.

b. *Public Area*: An open or common area where the expectation of privacy is not violated by what could normally be openly observed, such as the campus grounds,

hallways, classrooms, library, study rooms, computer labs, or residential common areas.

c. *Private Area*. Areas where an individual might change clothing, such as bathrooms, shower areas, locker and changing rooms. This would also typically include private office spaces; however, exceptions are appropriate in those areas where monetary transactions occur or where the use of CCTV is needed to safeguard money or supplies from theft, destruction or tampering.

d. *Video Surveillance Technology*: Any item, system, camera, technology device, communications device, or process, used along or in conjunction with a network, for the purpose of gathering, monitoring, recording, or storing an image or images of facilities and/or people. Images captured by video surveillance technology may be real-time or preserved for review at a later date. CCTV is one form of video surveillance technology.

e. *DRV:* Digital Recording Device is a hardware item that stores all captured video activity. Video is recorded to this device and once the DRV is at capacity all new activity replaces the oldest recorded information. Under optimal conditions all recorded information should be available for review for thirty (30) days.

IV. Application. The University recognizes the need to strike a balance between the individual's right to be free from invasion of privacy and the institution's duty to promote a safe environment for all community members. In light of this recognition, the University will use CCTV to enhance security, safety and the quality of life of the campus community by integrating the best practices of "virtual policing" with state-of-the-art technology. CCTV technology will extend the protection of the FAUPD, even when law enforcement officers are not in the immediate area. And, while not a guarantee of safety, CCTV is a tool that can be used to assist FAUPD personnel.

The purpose of CCTV surveillance at the University is three-fold: First, to promote a safe environment by deterring criminal acts; second, to assist in the identification of individuals who commit damage to University property; and third, to assist law enforcement with regard to the investigation of any crime that may be depicted. Video monitoring for security purposes will be conducted in a professional, ethical and legal manner. Personnel involved in active video monitoring will be appropriately trained in the responsible use of this technology.

The following uses of video technology are *not* prohibited or governed by this policy:

a. *Academic Use*. This policy does not apply to legitimate academic use of video cameras for educational purposes.

b. *Private Video Cameras*. This policy does not apply to private video cameras owned and operated by members of the campus community.

c. *Law Enforcement Surveillance*. This policy does not apply to cameras used covertly by law enforcement for criminal surveillance. This includes any portable hidden cameras or recording equipment used by the FAUPD for criminal investigations with approval of the Chief of Police.

d. *Unrelated to Surveillance*. This policy does not apply to video cameras or webcams established for reasons unrelated to surveillance activity, including without limitation remote monitoring of facilities construction to ascertain project progress, campus public relations initiatives or videotaping of athletic events for post-game reviews.

V. CCTV Installation and Placement. The Chief of Police shall propose recommendations to the Senior Vice President of Financial Affairs for the appropriate placement of video surveillance technology, taking care to ensure that the perimeter of view of fixed location cameras conforms to this policy. The Chief of Police, will also accept input and recommendations from members of the University community in reference to additional camera locations. The University's basic CCTV coverage for all new construction will provide for surveillance of the entire building's entry and exit points. Additional needs will be considered provided funding is available.

In proposing camera locations, the Chief of Police, shall be guided by the following rules governing placement of CCTV technology. Exceptions to these rules must be approved by the President.

a. *Public Areas*: Except when employed as a forensic tool by the FAUPD, video surveillance shall be restricted to public areas and areas commonly used by University community groups. These include, but are not limited to, the following areas:

- Alleys, service drives, and streets
- Athletic fields
- Audience seating
- Cash handling facilities
- Dining facilities
- Hallways
- Laboratories
- Library interiors
- Loading docks
- Malls, sidewalks, and other pedestrian walkways
- Parking lots
- Retail establishments
- Rooftops
- Safes

b. *Private Areas*: Video monitoring is limited to those areas where individuals would not have a reasonable expectation of privacy. Accordingly, except when specifically authorized, such as through the use of a search warrant, video surveillance shall not be approved in any of the following places:

- Individual residence hall rooms (without the occupant's permission)
- Public restrooms toilet stalls
- Public restrooms with urinals
- Individual offices (exceptions to include the obtaining of the occupant's permission and if the office is subject to narrow exceptions such as safeguarding of money, documents or supplies)
- Locker or dressing rooms (where showering or disrobing is routine)

c. *Residential Housing Views*: The Chief of Police shall ensure that camera positions and views of residential housing are limited. Any view of student housing will be no better than what is available with unaided vision. Furthermore, the view of a residential housing facility must not violate a students' reasonable expectation of privacy in that area.

d. The FAUPD will advise departments on the appropriate application of surveillance technologies.

e. *Changes in Law or Security Practices*: The Chief of Police shall monitor developments in the law and in security industry practices to ensure that camera surveillance is consistent with the best practices and complies with all applicable federal and state laws and regulations.

f. *Installation*: The FAUPD shall work with Facilities Planning and Information Technology Services to oversee the installation of all approved surveillance equipment.

g. *Objections to Camera Placement*: Where complaints are made about the location of video surveillance cameras, such as by students who believe their privacy is being infringed upon, the following process shall be followed:

- The Chief of Police will review complaints regarding camera locations and determine whether this video surveillance policy is being followed.
- The Chief of Police will make a determination as to whether the potential benefit in community security outweighs any likely infringement of individual privacy.
- In light of this determination, the Chief of Police, will make a recommendation to the Senior Vice President of Financial Affairs regarding disposition of the complaint.
- After a final decision regarding the complaint is reached, the complainant will be notified in writing of the decision.

VI. Monitoring. All University employees involved in video monitoring of public areas will perform their duties in accordance with the practices outlined in this policy. Specifically, the following guidelines shall apply to the monitoring of video surveillance cameras:

a. CCTV monitoring of campus areas for security purposes will be conducted in a manner that is professional, ethical, legal, and consistent with all existing University regulations and policies. Camera monitors shall monitor based on suspicious behavior, not individual characteristics. Monitoring individuals based on a person's race, gender, sexual orientation, national origin, disability or other protected characteristic is strictly prohibited.

b. *Restricted Access*. Video surveillance monitors shall not be viewable by unauthorized persons. No unapproved employees may monitor or view video or camera images for any reason except as necessary in the course of an investigation or adjudication. In furtherance of this expectation, the University will take reasonable security precautions to prevent unauthorized access to, use or disclosure of data monitored or recorded by any University surveillance systems.

c. *Viewing Access*. Access to video surveillance monitors will be limited. Specifically, the following guidelines shall apply in granting access to monitor the video surveillance cameras:

- FAUPD personnel will be permitted access to monitor all cameras at all times, regardless of location.
- Authorized Housing personnel will be permitted access to monitor all residential cameras at all times, regardless of location.
- Testing and evaluation representatives will be permitted access to monitor all cameras that capture images or areas that fall within their work area.
- Other faculty and staff personnel shall be permitted access to monitor all cameras that capture images or areas that fall within their work area or building location only with the written concurrence of their Department head and the approval of the Chief of Police.
- No other access shall be granted to any other members of the University community except as may be otherwise provided in this policy.

d. *Private Rooms or Areas*: Camera control operators shall not view private rooms or areas through windows.

e. *Intimate Activity*: Camera control operators will not spot and continuously view people becoming intimate in public areas.

f. *Audio Recordings*: The video surveillance systems used by the University will record video only. Audio recordings will not be authorized, unless specifically approved by the University's legal counsel.

g. *Evaluations of Employee Performance*: Video surveillance cameras will not be used by the University to evaluate employee performance or to monitor employees during their non-working time. However, surveillance camera may be used to monitor a student or employee work area, such as an area with financial transactions, even if there is only one student, faculty or staff member employed in that work area. Video surveillance camera used to monitor a work area will not be used to view the contents of computer screens.

h. *Community Requests*: Images captured by the University's CCTV system are subject to public record request and unless specifically exempted members of the community may request copies of recorded material. This request will be made to the FAUPD or the University's Press Secretary.

i. *Saving of Captured Information*: All persons who are authorized to view the CCTV system have the ability to save video images. All information that is saved must have the ability to be considered as evidence in reference to case development. Only personnel authorized by the Chief of Police may export captured information to DVD or other media.

Requests for exceptions to the guidelines listed above shall be made in writing to the Chief of Police. The request shall identify the individual for whom access is sought, the area to be monitored, and the rationale for why access should be granted. The decision to grant access will be made by the Chief of Police.

VII. Training. All personnel involved in the supervision, application, use or monitoring of video surveillance technology at the University must (i) be trained in the technical, legal and ethical parameters of appropriate camera use and (ii) receive a copy of this policy and provide written acknowledgement that they have read and understood its contents.

VIII. Storage. All recorded video should be available for review for a period of thirty (30) days from the date the recorded activity occurred. There will be times that due to the amount of cameras and/or activity being recorded to any particular DVR this time frame may be shortened.

IX. Release of Information. Information obtained through video monitoring will only be released when authorized by the Chief of Police, according to the procedures established in this policy. The following guidelines will govern dissemination of recordings obtained through the use of video surveillance technology:

a. Law Enforcement Purposes: Information obtained through video monitoring will be used for security and law enforcement purposes, and the FAUPD will cooperate and assist local police as requested with criminal investigations.

b. Commercial Use: Under no circumstances shall the contents of any captured video recordings be exploited for purposes of profit or commercial publication, nor shall such recordings be publicly distributed except as may be required by law.

c. Recordings Involving Active Criminal Investigations: Recordings directly related to active criminal investigations are exempt from Florida Public Records Requests and as such will not be released. Where requests for recordings take the form of subpoenas or other legal documents, appropriate liaison with the University's legal counsel is required.

d. All recordings should be considered evidence and all information exported to DVD must have a case number permanently attached or written on with permanent marker. If no case number will be assigned to information being exported to DVD the Chief of Police will be notified and approval must be obtained prior to the export of the information.

X. Destruction or Tampering with Video Surveillance Technology. Any person who tampers with or destroys a video surveillance camera or any part of the video surveillance system will be subject to appropriate administrative and/or disciplinary action, as well as possible criminal charges.

INITIATING AUTHORITY: Chief of Police

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: __1.11___

Initiating Authority
Signature: _____ Date: _____
Name: _____

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: _____

President
Signature: _____ Date: _____
Name: _____

Executed signature pages are available in the Office of the General Counsel