Video Electronic Surveillance Policy

1. Purpose & Introduction

1.1 The purpose of the SUNY Maritime College’s Video Electronic Surveillance Policy is to regulate the use of electronic video surveillance and recording of public and restricted areas for safety and security purposes.

1.2 SUNY Maritime’s video electronic surveillance is used exclusively for campus safety and security purposes and is administered and overseen by the Chief of University Police.

1.3 SUNY Maritime College respects the privacy of college community members and strives to balance privacy with the safety and security needs of the campus. Video surveillance cameras extend the protection of University Police, even when officers are not in the immediate area.

1.4 Video surveillance cameras are not a guarantee of safety or security, but are effective tools that assist University Police in their mission of maintaining campus security and protecting campus community members from dangers. Cameras also serve as deterrents to crime and they regularly expedite investigations.

1.5 The SUNY Maritime College Video Electronic Surveillance Policy applies only to campus owned video surveillance camera system and equipment.

1.6 This policy does not apply to covert cameras used by University Police for criminal surveillance as governed by the New York State Penal and Criminal Procedure Law.

1.7 The campus community and visitors are notified that cameras may be in use. Postings may accompany the cameras and/or be conspicuously posted at the entrances to the campus. The Video Electronic Surveillance Policy is disseminated and made available to all students, faculty, staff, and visitors and printed in appropriate publications.
2. Camera Placement

2.1 Temporary Video Surveillance Cameras are defined as cameras that are established by the University Police to provide additional safety and security for a campus event or a situation; they normally should not be in place for more than 30 days unless investigation or need determines an extended duration.

2.2 Permanent Video Surveillance Cameras may be established as part of the campus infrastructure and require planning and approval by the appropriate planning committee and University Police.

2.3 SUNY Maritime College has established a Video Surveillance Planning Committee to initially determine placement and use of Video Surveillance Cameras on campus. The Chief of University Police, in consultation with this committee, determines placement and use of cameras.

2.4 University Police may establish temporary or permanent video surveillance camera in public areas of the campus. These cameras will not make audio recordings.

2.5 The places where video surveillance cameras may be installed include public areas and specific, identified Restricted Access Sites such as departmental computer labs or data centers. No video surveillance cameras will be installed in private spaces (defined as areas where a person has a reasonable expectation of privacy) including residence hall rooms, bathrooms, lavatories, showers, locker and changing rooms, medical and treatment areas (except cameras possibly used narrowly to secure money, documents, supplies or pharmaceuticals from theft, destruction or tampering).

2.6 In an effort to combat repeated or suspicious criminal acts or safety issues (either by deterring the activity or apprehending the violators) SUNY Maritime College University Police may use video cameras for covert surveillance purposes. Any such use will be governed by the New York State Penal and Criminal Procedure Laws.

2.7 Video Surveillance Cameras shall not be directed or zoomed into the windows of any private residential building or office. To the maximum extent possible, electronic shielding will be placed in the camera so that the camera does not have the capability to look into or through windows.

2.8 Video Surveillance Cameras may be directed or zoomed into doors of residential and non-residential buildings for monitoring and recording of public areas within these spaces. These spaces include residential lobbies, common areas, lounges, etc.

2.9 SUNY Maritime College strongly discourages use of empty, dummy, or placebo cameras due to liability concerns and the undermining of the deterrent function of the surveillance system.
3. Camera Use and Non-Use:

3.1 Video surveillance cameras are used exclusively for campus safety and security purposes. No cameras will be used to monitor individual students, faculty, or staff (except as necessary and described in section 2.6, for a criminal surveillance/investigation and except as in accordance with the New York State Penal and Criminal Procedure Laws).

3.2 Cameras may be used to monitor student or employee work areas. Cameras used to monitor work areas are not intended to view the contents of computer screens unless a specific security, safety, policy or investigative purpose outlined in Section 1 exists.

3.3 The College will not use video surveillance cameras to prosecute parking violations, including parking rules, unless review of a formal complaint results in a determination that a campus safety or security issue exists.

4. Camera Monitoring:

4.1 Live images and recordings may only be monitored or reviewed by University Police or the Information Security Specialist on duty.

4.2 No students may be hired to monitor, record or view images or video.

4.3 All video images recorded, and all information and/or observations derived from the use of College video surveillance cameras is considered confidential and can only be used for official business.

4.4 UPD officers and Information Security Specialists will receive a copy of this policy and provide written acknowledgement that they have read and understand this policy and will receive any and all updates or amendments to this policy and will confirm acknowledgement of those with a written receipt.

4.5 UPD officers and Information Security Specialists will receive appropriate and ongoing training on the campus video surveillance systems and the appropriate use of same.

5. Storage Media:

5.1 Recordings will be stored in a manner consistent with available technology and transported in a manner that preserves security. Current and archived recordings will be kept locked and secured.

5.2 A log will be maintained by UPD of archived recordings.
5.3 Recordings not related to, or used for, an investigation will be kept strictly confidential and destroyed in accordance with a retention policy, based on storage capabilities and need. Recordings or images used for investigation or prosecution of crime shall be retained until the end of the court or judicial proceedings and appeal period unless directed otherwise by a court.

5.4 Any attempt to alter any recording is strictly prohibited. Editing or otherwise altering recordings or still images is only permitted to enhance quality for investigative purposes, place a watermark, reduce size for transport or blur features to protect privacy. Unauthorized editing or tampering will be prosecuted to the fullest extent of the law.

5.5 Transmission of recordings using the Internet or campus network will use appropriate safeguards to ensure that recordings are not improperly accessed or vulnerable to inadvertent disclosure. University Police will work with the Department of Information Technology staff to establish security for the video surveillance system and to ensure proper password and encryption technology for recordings or images transferred or transmitted over the internet or on the campus network.

6. Destruction or Tampering with Cameras

6.1 Any person who tampers with or destroys a video surveillance camera or any part of the electronic surveillance system (including wiring) will be prosecuted in the criminal justice system, as well as the campus judicial system.

7. Further Information

7.1 Further information about the Electronic Surveillance Policy can be obtained by contacting SUNY Maritime College’s University Police at 718-409-7311.
Electronic Surveillance Policy

Acknowledgement

By signing below, I acknowledge that I have received and read the SUNY Maritime College Electronic Surveillance Policy.

I further acknowledge that I must comply with this policy and failure to abide by this policy can result in revocation of resources, disciplinary action, written or verbal warnings, recovery of damages, suspension, termination, and/or referral to appropriate state and federal authorities for investigation.

Name: ______________________________ Date: ____________________

Signature: ______________________________________________________