University of the Incarnate Word
Video Security Applications

Effective Date: **February 28, 2018**
Contact: Sam McDaniel, Dir EHSRM, Environmental Health and Safety

PURPOSE

To govern the use of Video Security Applications on campus properties.

SCOPE

This policy applies to all campus properties owned, leased or controlled by the University of the Incarnate Word. Video security applications shall serve two purposes:

- If an area is posted as being under video monitoring or surveillance, video security applications can be a crime deterrent.
- Once a crime has been committed, the video security applications can assist in the identification of the responsible parties.

DEFINITIONS

Camera Control Operator: anyone who operates, views, or reviews video security application images. Typically, this will be a UIW Police officer or EHSRM employee.

Video Security Application: any device or component that captures images (with or without sound). Examples of video security applications include closed-circuit television (CCTV), video cameras, web cameras, still cameras, and any electronic means to store and review their images.

OFFICE OF ENVIRONMENTAL, HEALTH, SAFETY, & RISK MANAGEMENT

This policy shall be administered by the Office of Environmental, Health, Safety, & Risk Management (EHSRM). All Video Security Applications shall conform to federal and state law in addition to standards established by EHSRM.

USE

EHSRM shall review, recommend, approve, and manage proposed and existing video security applications. To ensure the ability to use the data, the equipment and systems shall be standardized and accessible to EHSRM, Human Resources, Title IX Coordinator and law enforcement authorities upon request. ESHRM shall maintain a list of all video security applications. ESHRM shall also:

- Document the release of any video security applications data.
- Periodically review this policy and update as necessary.

Information obtained through video security applications is primarily for security and law enforcement purposes, and compliance with university policies. Information may also be approved by ESHRM for other purposes, including, proceedings for employee and student disciplinary investigations, civil claims or lawsuits where the recording are relevant or may be subpoenaed.

Releases of video security applications data shall be released and authorized only by ESHRM or the Chief of Police. No other campus unit may release data obtained through video security applications.

GUIDELINES

1. Video monitoring for security purposes must be conducted in a professional, ethical, and legal manner. Personnel involved in monitoring will be appropriately trained and supervised in the responsible use of this technology.
2. Video monitoring is not permitted to view or record personal living and private areas where there is a reasonable expectation of privacy. EHSRM will not approve camera locations with views of interior residential spaces, with the exception of the use of video monitoring for criminal investigations where the focus of the cameras will not cover areas where there is an expectation of privacy. This does not preclude monitoring the exterior of buildings or building lobbies.
3. Camera control operators and/or managers of video security applications will monitor based on suspicious behavior, not individual characteristics. Monitoring will be conducted in a manner consistent with all University policies, including the Non-Discrimination Policy, the Sexual Harassment Policy, Sexual Misconduct Policy and other relevant policies. Camera control operators will not monitor individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other classifications protected by the University's *Non-Discrimination Policy*.
4. Camera control operators of video security applications will not seek out or continuously view people being intimate in public areas.
5. Camera control operators will be trained in the technical, legal, and ethical parameters of appropriate camera use. Camera control operators and/or managers of video surveillance applications will receive a copy of this policy and will provide written acknowledgement that they have read and understand it. Failure to provide acknowledgement does not excuse violation of this policy.
6. EHSRM and UIW Police are authorized to use still cameras or video equipment to record events where there are likely to be violations of state or federal laws, university policies or violations of the law. Cameras may be operated either overtly or covertly depending on the circumstances. In the case of demonstrations, protests, and similar situations, cameras may be permanently mounted or operated from either remote locations or by automated devices.
7. The following signage may be required by EHSRM and UIW Police at public locations monitored by video surveillance:

"THIS AREA IS SUBJECT TO VIDEO RECORDING

For more information, contact <u>XXXXXXX at XXX-XXX-XXXX</u>"

An exception to the use of signage would be if announcing the use of video surveillance would undermine its purpose.

8. Dummy cameras <u>will</u> NEVER be used, as they could lead the viewer to a false sense of security that someone is monitoring the cameras.
9. Campus departments approved by EHSRM to operate and manage video surveillance systems will make available to EHSRM and UIW Police the recorded video tapes or permit access to their application via the campus network for maintenance, auditing, and police investigations.
10. Recorded images will be stored in a secure location with access by authorized personnel only.
11. Recorded images will be stored for a period of no less than 30 days before they are erased. Recordings may be retained longer if they are subject to a litigation hold, subpoena, or request by law enforcement by law enforcement authorities.
12. Installation of video security applications are the budgetary responsibility of the requesting department. This responsibility includes the cost of IP addresses, service, and maintenance.

13. At least five business days' notice must be provided to EHSRM prior to changing the connectivity, digital storage, or IP address for a video system.

Implementation of this policy for all existing uses of video monitoring and recording is within 6 months of the policy's date.

Web Site Address for This Policy:

uiw.edu/safety/videosecuritypolicy

First Approved: February 28, 2018
Revised:
Revised: