

Handbook of Operating Procedures

VIDEO SECURITY APPLICATIONS

A. Purpose

The University of Texas Rio Grande Valley (UTRGV) is committed to protecting the safety and property of the UTRGV community, while also respecting the reasonable expectation of privacy of our faculty, staff, students, and visitors. The purpose of this policy is to provide the requirements and procedures for the installation, recording, handling, viewing, dissemination, retention and destruction of video security records.

B. Persons Affected

Employees, faculty, contractors, or vendors in any campus unit that uses video for the purpose of safety or security.

C. Policy

1. Campus units and employees, faculty, contractors or vendors may not use video security applications without the prior review and approval of the UTRGV Police Department (UTRGV PD). Campus units requesting permission to use video security applications must demonstrate that the application serve purpose(s) such as:
 - a. Deterrence or Detection: The presence of video security application may dissuade a potential perpetrator from attempting a crime, or use of the application may alert human operators to abnormal conditions that can increase likelihood of prevention or apprehension of suspects.
 - b. Response: When an alarm is raised, an incident is detected, or an incident is reported, an operator can use the video security system to view the location and assess the situation before responders arrive.
 - c. Investigations: After a crime has been committed, recorded video may reveal images pertinent to the investigation of the crime. These images may be immediately shared with local law enforcement personnel, assisting with the rapid identification of suspects or the recovery of valuable property.
 - d. Situational Awareness: The ability to monitor real-time video can lead to the detection of developing situations that may become a threat to campus safety and security.
2. This policy does not apply to video recording or monitoring used for operational purposes (e.g. video conferencing), academic purposes, media purposes or recording of public performances, events, or interviews provided that such activity is disclosed or readily apparent to those in view of the camera. Examples of such excluded activities would include videotaping of research subjects, athletic events for post-game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons.
3. Information obtained through video security applications will be used primarily for security and law enforcement purposes. However, UTRGV may also use information from video

- security application in support of other legitimate purposes, including disciplinary proceedings involving faculty, staff, or student(s), or in a civil lawsuit involving person(s) or activities that are shown on the recording and are the basis for the suit.
4. Video monitoring for security purposes is expected to be conducted in a professional, ethical, and legal manner. Violations of this policy or procedures may result in disciplinary action consistent with UTRGV and University of Texas System rules and policies.

D. Procedures

1. Responsibilities:

a. *Capital Projects:*

- i. UTRGV Facilities Planning & Operations and the UT System Office of Capital Projects must coordinate with UTRGV PD in the selection and installation of video security applications in new construction. Video security applications may not be installed in new construction unless first reviewed and approved by the UTRGV PD.

b. *Campus Departments:*

- i. Campus units with existing video security applications must have their applications reviewed and approved by the UTRGV PD.
- ii. Campus units that wish to install new video security applications must submit their plans to the UTRGV PD for review and approval before acquisition and installation may proceed.
- iii. Department heads or their designees charged with overseeing video security applications must arrange for UTRGV PD to manage their video security applications.
- iv. Campus units should carefully consider who may be viewing video monitoring as judgment and ethical behavior are important relative to individual privacy concerns.
- v. Each campus unit with legacy video security application platforms must provide the UTRGV PD with an emergency personnel list that can be contacted during business and after hours to access the video security application platform.

c. *UTRGV PD:*

- i. UTRGV PD will timely review requests for video security applications and oversee the installation, servicing, and management of approved video security applications.
- ii. UTRGV PD will monitor developments in relevant laws and in the security industry to assure that video monitoring on UTRGV property is consistent with the highest standards and protections.
- iii. UTRGV PD will Maintain a list of all University-owned or -controlled camera locations.
- iv. Requests for the release of recordings obtained through video security applications must be timely processed in coordination with UTRGV PD.
- v. Any request for the release of any video security application footage will require a request to the Chief Legal Officer, Public Information Officer, or Chief of Police (or

designees). No campus unit or UTRGV PD designee may release video security application footage without the permission of the Chief Legal Officer, Public Information Officer, or Chief of Police (or designees).

vi. UTRGV PD will document the release of any video security application footage.

vii. UTRGV PD will periodically review this policy and update as necessary.

d. *Camera control operators or managers of video security applications:*

i. Camera control operators or managers of video security applications are expected to monitor based on suspicious behavior, not individual characteristics. Monitoring will be conducted in a manner consistent with all existing UTRGV or UT System policies, including without limitation UTRGV HOP Policies [ADM 03-100 Non-Discrimination and Complaint Procedure](#), [ADM 03-300 Sexual Misconduct](#), and other relevant policies.

ii. Camera control operators or managers of video security applications should not seek out or continuously view people being intimate in public areas.

iii. Camera control operators or managers of video security applications should not continuously view private offices or living areas.

iv. Camera control operators must be trained in the technical, legal, and ethical parameters of appropriate camera use. Camera control operators or managers of video surveillance applications must be provided a copy of this policy and must provide written acknowledgement that they have read and understood the policy. Failure to provide written acknowledgement does not excuse any policy violation.

v. Camera control operators may not use other recording devices to capture security camera video footage.

2. Permissible methods and locations for video security application use:

a. UTRGV PD is authorized to use still cameras or video equipment to record events where there are likely to be violations of UTRGV or UT System rules, regulations, policies, or violations of law. Cameras may be operated either overtly or covertly depending on the circumstances. In the case of demonstrations, protests, and similar situations, use of cameras generally will be overt, partly as a means of deterring illegal acts. Cameras may be permanently mounted or operated from either remote locations or by automated devices.

b. UTRGV generally will not use dummy cameras, as they could lead the viewer to a false sense of security that someone is monitoring the cameras.

3. Non-permissible methods and locations for video security application use:

The focus of cameras used in video surveillance generally will not cover areas where there is a recognized expectation of privacy. The UTRGV PD will not approve camera positions with views of residential spaces, with the exception of the use of video monitoring for criminal investigations, pursuant to a warrant if deemed necessary. This does not preclude monitoring the exterior of buildings or building lobbies.

4. Storage, access, and retention of video security application recordings:
 - a. Recorded images must be stored in a secure location with access by authorized personnel only. Designated police personnel from the Criminal Investigation Division, Community Engagement Unit, the Office of the Chief of Police, and patrol officers conducting preliminary criminal investigations will have access to the video/digital recordings.
 - b. Recorded images will be stored for a reasonable period of time consistent with business purposes and should then be erased or deleted in compliance with applicable records-retention policies, unless retained as part of a criminal investigation or court proceeding (criminal or civil), or other use as approved by the Chief of Police or designee.
 - c. Cameras are not normally set up to record audio. In the event that audio is recorded, it will be handled in the same manner as video.
 - d. Only the Chief Legal Officer, Public Information Officer, the Chief of Police, or their designee(s) may release data produced by video security applications.
5. Campus Units with existing video security application data platforms will make available to UTRGV PD the recorded footage or permit access to their application via the campus network for maintenance, auditing, and police investigations. Existing video security application platforms must be brought into compliance within twelve (12) months of the policy's effective date.
6. Installation of video security applications are usually an institutional responsibility that require approval from the responsible vice president over administration support services. However, the School of Medicine, Auxiliaries and Grant Projects will be financially responsible for the installation, service, and maintenance of their respective video security applications.
7. At least five (5) business days' notice must be provided to UTRGV PD prior to changing an IP address for a video system.
8. To maintain an informed UTRGV community, UTRGV PD will periodically disseminate written materials describing the purpose of video monitoring and the guidelines for its use. The use of outdoor/indoor video cameras will be published in the Annual Security Report.

E. Definitions

1. Camera Control Operator – anyone who operates, views, or reviews video security application recordings. Typically, this will be a UTRGV PD employee or UTRGV PD designee.
2. UTRGV PD Designee – any person(s) authorized by UTRGV PD to view or review video security applications.
3. Video Security Application - any device or component that captures images (with or without sound) for the purpose of deterring unlawful behavior or identifying the perpetrators of unlawful behavior. Images may be viewed immediately and/or kept on a storage device. Examples of video security applications include closed-circuit television (CCTV), video cameras, web cameras, and still cameras.

F. Related Statutes or Regulations, Rules, Policies, or Standards

[ADM 03-100 Non-Discrimination and Complaint Procedure](#)
[ADM 03-300 Sexual Misconduct](#)

G. Dates Reviewed or Amended

Not applicable.