TEXAS TECH UNIVERSITY™

Operating Policy and Procedure

OP 61.45: TTU Security Video Operations

DATE: February 22, 2022

PURPOSE: The purpose of this Operating Policy/Procedure (OP) is to define and outline procedures for the campus use of security video systems for security purposes.

REVIEW: This OP will be reviewed in July of odd-numbered years by the Associate Vice President for Operations Division, the Texas Tech Chief of Police, the Chief Information Officer (CIO) and Vice President for IT, the General Counsel, and the Senior Managing Director of Facilities Maintenance & Construction for Operations Division, with substantive revisions forwarded to the Senior Vice President for Administration & Finance and Chief Financial Officer.

POLICY/PROCEDURE

1. Texas Tech University may use security video systems to enhance safety and security, while respecting the privacy rights of the university community.

a. This operating policy does not imply nor ensure that security camera equipment is present, operational, monitored, or recorded.

2. The Texas Tech Chief of Police has oversight of all video security systems.

3. The operation, management, and installation of all video security systems are managed by the Operations Division. Camera views will be reviewed on a regular basis to ensure proper operations.

4. The administration and monitoring of all video security systems shall be conducted by the Texas Tech Police Department or through an authorized third party where applicable.

a. All security video systems and any and all recordings made available and stored for the safety and security of the Texas Tech University community and property belong to and are solely for the use of Texas Tech University and the appropriate personnel as outlined in this policy.

b. All security video systems used by event contractors that lease space from the university including bookstores, banks, and food services belong to and are solely for the use of Texas Tech University and the appropriate personnel as outlined in this policy.

5. Exceptions

The following are excluded from this policy:

a. Video conferencing systems, including web cameras connected directly to a computer;

b. Video conference systems used in campus vehicles that are publicly visible to passengers and driver;

c. University-sanctioned event recording, including athletics and performing arts events;

d. Student Union & Activities, recreational sports, United Supermarkets Arena, and housing events;

e. Lecture and instructional recordings;

f. Video cameras used in teaching, learning, and sanctioned research projects;

g. Cameras used for monitoring digital signage operations; and

h. Texas Tech Police Department body camera or in-car video systems.

i. When deemed necessary, surveillance systems used in areas without internet or electrical access or temporary security video systems may be used through the approval of the Texas Tech Chief of Police.

All other exceptions to this policy must be approved in writing by the Associate Vice President for Operations Division and the Texas Tech Chief of Police.

6. Equipment

All network video cameras and recorders used for safety and security must be approved in writing by the Associate Vice President for Operations Division and the Texas Tech Chief of Police.

7. Policy

a. The policy applies to all Texas Tech University faculty, staff, students, and visitors with respect to the installation and use of security video systems in facilities owned or controlled by the university, including auxiliary or off-campus sites.

b. The policy governs all new security video systems installed after January 1, 2020.

c. All security video systems in use prior to July 2019 must have an exemption on file, be approved through the Texas Tech Chief of Police, removed, replaced, and/or upgraded to comply with this policy by August 31, 2025. Systems currently in use by Student Housing, Hospitality Services, and Transportation & Parking Services are exempted. Any new equipment purchases must comply with this policy.

d. The installation and use of all security video systems must adhere to applicable state and federal laws.

e. All purchases of video security systems and recording equipment are subject to procurement review by the Office of the Senior Managing Director of Facilities Maintenance & Construction, the TTU Office of the CIO, and the Texas Tech Police Department.

f. Authorized personnel must be adequately trained to use, operate, maintain, and monitor security video systems, and must clear a Level II security clearance as referenced through OP 70.20, Employment for Security-sensitive Positions.

g. Video retrieval/viewing shall be kept to a minimum number of authorized personnel to maintain the process integrity. Departments must each maintain a list of authorized personnel, who must be approved by the Texas Tech Police Department.

h. The use of fake, decoy, or inoperable video camera equipment is prohibited.

8. Intended Use

a. The use of video monitoring governed by this policy is for enhanced safety and security. Any use other than those outlined in this policy is prohibited.

(1) In accordance with state and federal laws and in situations as deemed appropriate, proper monitoring notification will be provided.

b. Monitoring or recording of audio is strictly prohibited.

(1) Exception may be granted on a case-by-case basis by the Texas Tech Chief of Police.

c. Monitoring and recording shall be limited to uses that do not violate a reasonable expectation of privacy.

d. Any dissemination of video shall be authorized by the Texas Tech Chief of Police before public release, unless otherwise required by law.

9. Retention

Recordings must be maintained for a minimum of 30 days and a maximum of 60 days unless required as part of a criminal investigation or court proceeding (civil or criminal) or other authorized use as approved by the Texas Tech Chief of Police.

10. Device Security

a. All systems, regardless of use, connected to the university network must comply with TTU IT Security Policies as referenced through OP 52.04, Information Technology (IT) Security, and Telecommunications Standards and Controls as referenced through OP 52.03, Telecommunications Services.

b. All default passwords must be changed in accordance with the TTU Password Policy as referenced through OP 52.04, Information Technology (IT) Security.

c. Security patches and updates must be applied within one month of release or by the date recommended by the manufacturer, whichever is earlier.

d. All insecure or unused protocols and services (software programs) must be disabled in accordance with OP 52.04, Information Technology (IT) Security. For assistance, contact Enterprise IT Security at security@ttu.edu.

e. All security camera video transported over a network must be encrypted with the current industry standard.

f. Security camera systems must not be directly accessible from the internet.

11. Maintenance and Support

Departments must maintain annual maintenance and support and pay any associated costs, except for the areas exempted by the Associate Vice President for Operations Division.

12. Contacts

- Operations Division – Work Control – 806.742.4677 (4OPS) (https://webtma.operations.ttu.edu:8080/home.html)
- IT Division – 806.742.5151 (www.it.ttu.edu)
- Texas Tech Police Department – Communications – 806.742.3931 (http://www.depts.ttu.edu/ttpd/)

13. Requests

a. Equipment

All requests for security video systems must be submitted to Operations Division's Work Control at https://webtma.operations.ttu.edu:8080/home.html or by calling 806.742.4677 (4OPS). Operations Division coordinates with the Texas Tech Police Department to design and install.

b. Video Recording

Approved personnel, in accordance with sections 7.f. and 7.g. of this OP, may retrieve and view video recording as necessary within their area of oversight. Temporary access may be granted on a case-by-case basis through the Texas Tech Chief of Police.

14. Right to Change

Texas Tech University reserves the right to interpret, change, modify, amend, or rescind this policy, in whole or in part, at any time without the consent of employees or students.