

Audio Visual Surveillance Technology Operational Standards

Table of Contents

General.....	1
Authorized Users.....	2
Camera Operation and Location.....	2
Appropriate and Inappropriate AVST Use	3
Signage for AVST Equipment	4
Changes in AVST Location or Purpose	4
Security of AVST	4
Appropriate Handling of AVST Material	4
Access and Monitoring of AVST	4
Reviewing Recorded AVST Material.....	5
Release of AVST Material.....	5
Retention of Recorded AVST Material.....	5
Oversight of Surveillance Equipment Purchases	5
Requests for Installation of Equipment	6
Required Training for AVST Authorized Users.....	6
Complaints and Questions Regarding AVST.....	7

General

Audio video surveillance technology may be used by Texas A&M University and other System Member agencies located in College Station to enhance security of state property, facilities, and people as authorized by university rules and standard administrative procedure 29.01.99.M1.28, Information Resources – Security Surveillance.

The following standards are for installation, relocation and use of approved AVST equipment and the circumstances in which recorded material may be reviewed or released.

Audio video surveillance technology (AVST) includes all types of cameras and/or receiving audio devices placed in operation internally or externally throughout campus (i.e., surveillance devices that are located on or provide surveillance of TAMU facilities, or are connected to the TAMU network) and the related equipment to operate the cameras/audio or view, listen, and record images and/or audio. All

uses/placement of AVST equipment must be reviewed and approved by the AVST Committee, excluding the following purposes:

- a) authorized broadcast media: (Examples: television cameras for news reporting, sports broadcasts, public performances, etc.);
- b) used for online communication/meetings between remote locations; (Examples: video conferencing or video collaboration)
- c) academic/instructional; (Examples: authorized academic research, instructional support, performance or coaching activities not otherwise subject to these standards);
- d) investigatory (managed by law enforcement officers or official auditors); **Or,**
- e) other non-surveillance/non-monitoring uses where any person being viewed and/or recorded via the technology is either:
 - i. an informed and willing participant; or
 - ii. not identifiable through the use of the technology.

(Examples of such uses could include sensors/counters, art installations, performance development, and multi-media creations).

The AVST Committee reserves the right to review, for committee compliance requirements, any of the above installations and/or uses of AVST equipment.

AVST equipment used for surveillance may be monitored or non-monitored.

Authorized Users

All AVST equipment and operations must be administered by authorized users within the department or unit installing such equipment. Authorized users are generally considered to be the designated employees who handle the operations, maintenance, and/or have direct/independent access to AVST equipment and/or recorded data. All authorized users will complete training on operations and appropriate use of AVST. They will acknowledge their responsibility and willingness to comply with the AVST Ethics Statement as presented in the online training course ([TRAINTRAQ - 2111557 : Audio Visual Surveillance Technology \(AVST\) Operations Training - NIS](#)).

Camera Operation and Location

All new installations or relocation of surveillance cameras and related equipment must be approved prior to installation by the Audio Video Surveillance Technology Committee as authorized by university Standard Administrative Procedures.

The monitoring of people must only be for suspicious behavior or authorized observation functions (e.g., Becky Gates Children's Center). Monitoring that is based on perceived individual characteristics or protected classifications including race, gender, ethnicity, sexual orientation, or disability is prohibited. Surveillance cameras may be installed in such areas as the following:

- Those containing such security systems as the following:
 - Access control systems, which monitor and record restricted-access transactions at entrances to buildings and other areas

- Security alarms, including intrusion alarms, exit-door controls, hold-up alarms, cashier locations, etc.
- Those containing sensitive institutional data or technology operations
- Sections of the university campus and buildings that are high-traffic, such as shopping areas, perimeters, unrestricted entrances, exits, lobbies, corridors, and receiving docks
- Those housing sensitive operations, such as storage areas for special materials, laboratories, select agents, etc.
- Those containing rare, high-value, or merchandise property, such as the University Library Rare Book Collections and the University Store

Cameras intended for monitoring or displaying general access to public events must be approved in advance and privacy concerns must be specifically addressed by the department requesting approval.

Surveillance cameras must not be located in or monitor a campus housing resident's room or restroom/shower area, or any other restroom/shower area where there is a reasonable expectation of privacy. These types of facilities are used by individuals with a reasonable expectation of privacy and should not be monitored or recorded by a surveillance camera.

Surveillance cameras may be used at times for investigating criminal activity. These types of installations are generally temporary and are managed by the University Police Department. Authorized operators and administrators of AVST equipment in a department may be asked to cooperate and assist official UPD investigations.

AVST technology should not be used as a tool for routine performance management of employees or academic performance of students.

Inoperable cameras should not be installed at any location as a "dummy" cameras intended to appear as operable.

Appropriate and Inappropriate AVST Use

Surveillance camera use is considered **appropriate** when it enhances:

- The protection of equipment, facilities, and individuals
- The protection of sensitive institutional data or technology operations
- Instruction or research in the classroom or lab
- Protection of property/persons by monitoring of building entrances and exits
- Operational Use – in support of routine authorized procedures where the AVST monitoring replaces or augments an on-site-observer that would be necessary for the effective execution of the operation.

While observation of people may be an incidental extraneous consequence in the observation of certain locations, operations, or assets, intentional observation of people would not be considered "operational use" except in specific situations (e.g., where preventive safety is an issue or such observation is essential to the execution of the operation).

Examples of routine operational use would be the Becky Gates Children’s Center, and the support/monitoring of transportation and traffic operations.

Surveillance camera use is considered **inappropriate** when it entails:

- Infringement on a person’s reasonable expectations of privacy
- Monitoring of personnel related issues or performance not involving safety
- Monitoring of student performance for academic dishonesty
- Installation of a “dummy” camera for appearance sake

Signage for AVST Equipment

Conspicuous, public signage (signs of such size and/or location that would be difficult to be overlooked by the average person) must be displayed at all main entrances of buildings and facilities with AVST equipment or in the immediate area of the equipment. Surveillance cameras in some locations may be actively monitored in real time by authorized personnel, whether sporadic or continuously, while other camera locations may not be monitored at all. Departments must avoid creating a false sense of security and clearly indicate in their posted signage if their AVST equipment is not continuously monitored. Signage of the approved size and with approved language is available from the Texas A&M University Facilities Services, Graphics Shop as follows:

“This area is subject to electronic surveillance and may or may not be actively monitored.”

Changes in AVST Location or Purpose

If it is desired to change the location (i.e., a different surveillance space/room) of an approved AVST installation, approval must be requested from and granted by the AVST Committee based on the new location and purpose of the equipment. If the rationale upon which an approval was based becomes invalid or is no longer applicable, a new approval must be requested and granted or the AVST equipment must be removed. The AVST committee must also be informed if a department decides to remove AVST equipment (email - avst@tamu.edu).

Security of AVST

Units administering AVST equipment must establish monitoring locations and physical security measures to prevent accessing or tampering with monitoring equipment and recorded surveillance material by unauthorized users. Cameras and similar technologies must have sufficient security measures, such as encryption, to prevent unauthorized access to the output of the equipment. Access must require authentication over a secure channel, such as SSL. Encryption of video output is not a requirement at this time, but reasonable measures should be taken to mitigate interception.

Appropriate Handling of AVST Material

AVST activity, information, data or recordings should be treated as sensitive and handled appropriately at all times. Authorized users assigned to monitor live camera video displays, whether for operational or

maintenance procedures, or for surveillance have a responsibility to perform these duties following all policies, regulations, rules and SAPs governing any employee activity.

Access and Monitoring of AVST

Other than what is necessary to maintain the operational reliability and security of the AVST system, recorded surveillance material will not be accessed or released except in the event of an official investigation/request process as prescribed by law, regulations, rules, or standard administrative procedures and directed by appropriate university officials or law enforcement officers.

In accordance with applicable federal and state law and in support of Texas A&M University rules prohibiting discrimination and harassment, recordings and monitoring of activity through AVST equipment will not be based on the subjects' race, color, national or ethnic origin, religion, sex, disability, age, sexual orientation, veteran status or any other protected characteristic.

Reviewing Recorded AVST Material

Requests to review AVST data or recordings must be approved in advance by the information resource owner and in response to official business needs or official/documented investigative procedures (see following paragraph). The data or recordings may only be directly accessed by the documented data owner or by employees whose duties include administration of the AVST equipment. All persons accessing/reviewing AVST data or recordings must have completed training which includes their acknowledgement to abide by the ethics statement.

Internal review generally follows the appropriate reasons and procedures for the release of AVST material. Appropriate reasons for internal review include an internal investigation of a report of missing property, formal investigation of a documented allegation of misconduct, or an event resulting in personal injury or property damage. Access or review of AVST material is not appropriate to determine attendance, settle disagreements, or investigate employee or student behavior not related to a formal allegation of misconduct or a reported threat to safety. All access or reviews of AVST material are to be documented individually unless such access/review is part of routine documented operational use or in support/maintenance of the AVST system. Documentation is to include the reason for the access/review, person(s) performing the review or access, a description of the material accessed/reviewed, and any result or conclusion of the access/review.

Release of AVST Material

Requests for the release of AVST data or recordings must be approved in advance by the information resource owner, unless the release is required by federal or state law. The data or recordings may only be released following established procedures for the release or disclosure of information such as an official complaint process, investigations by authorized university officials¹, subpoenas or court orders, or public

¹ A University or Texas A&M System employee or agent whose duties within the course and scope of their employment or agency include a responsibility of inquiry/investigation regarding matters presented.

information requests. All requests, approvals and releases of data or recordings must be documented and maintained by the department managing the AVST equipment.

Retention of Recorded AVST Material

Recorded surveillance material should be stored in secure locations accessible only to designated individuals. Such records are considered to be transitory information and retained for no less than fourteen (14) days and no longer than thirty-one (31) days. Records preserved for longer than 31 days related to an official investigation or court proceeding are to be deleted when no longer needed for the investigation. Surveillance material kept by UPD is an exception to this requirement.

Exceptions to this retention period must be approved in advance by the Vice President and Associate Provost for Information Technology or designee. Documented retention periods for existing equipment that cannot meet this requirement must be submitted to the Vice President and Associate Provost for Information Technology or designee.

Oversight of Surveillance Equipment Purchases

The AVST Committee will utilize the university's AggieBuy system to support oversight responsibilities of surveillance equipment by being alerted when related equipment defined by specific commodity codes is purchased or paid for through AggieBuy.

The AggieBuy system includes online catalogues by which authorized users may select, order, purchase, receive and approve payment for business-related equipment and supplies. Products are identified by a commodity code which may be flagged for notification to specific individuals to review and approve or be notified of activity in AggieBuy.

The AVST Committee designee(s) will be notified through AggieBuy when the following commodity codes are used for purchases:

46171610 – Security cameras (5752 and 8424)

46171612 – Video monitors (5752 and 8424)

46171615 – Light enhancing cameras or vision devices (5752 and 8242)

92121701 – Surveillance or alarm maintenance or monitoring (5672)

The notification or information within AggieBuy will provide contact details of the items purchased, the purchasing department and the purchaser's name, telephone number and email. The committee designee will evaluate if the purchasing department has already submitted and received approval for surveillance equipment; if not, the designee may contact the purchasing department's employee or department head to discuss procedures for installation requests.

Requests for Installation of Equipment

All new installations and relocations of AVST equipment must be submitted through the AVST Committee for review and recommendation according to SAP 29.01.99.M1.28. Notification must be submitted to the AVST committee if a department removes previously installed AVST equipment. The committee reviews requests for appropriate use and location, adherence to university standards and guidelines, and appropriate administration of AVST equipment and data. The committee's recommendations are submitted to the Vice President and Associate Provost for Information Technology for final determination of the request.

Approval of installation and relocation requests will be guided by the need for security of state property, facilities and people, with attention given to the privacy of members of the university community. It is strongly recommended that unbiased security surveillance expertise be consulted regarding the use/need and location of any AVST devices prior to the submission of a request in order to promote the effective and efficient use of AVST resources.

The online installation request form and instructions are available at [AV Surveillance \(http://cio.tamu.edu/Risk_Management_Policy/Risk_Management_and_Compliance/Compliance/AV_Surveillance.php\)](http://cio.tamu.edu/Risk_Management_Policy/Risk_Management_and_Compliance/Compliance/AV_Surveillance.php) and can be submitted by email to avst@tamu.edu. The individual listed as the primary contact will be notified by email for more information before responding to the request or giving approval to proceed with the installation. The request form must be signed by the dean/department head/director or documented designee. (The AVST Ethics Statement is also available at the above URL.)

The approval process may take several weeks to complete depending upon the details of the request and supporting materials, or concerns by the committee. Requesting departments should build into their installation timelines sufficient time for the AVST committee to submit recommendations to the Vice President and Associate Provost for Information Technology for final determination of the request.

Required Training for AVST Authorized Users

Authorized users of AVST, (e.g., employees who operate or maintain AVST and/or have direct/independent access to AVST equipment and/or recorded data or live view) must complete training before installation of equipment or within 30 days of approval from the AVST committee for installation. The training developed by the AVST committee which covers information in these standards and ethical use of AVST, is offered online in the university's TrainTraq system. Departments with AVST equipment must assign the training course and monitor completion of employees identified as authorized users. Employees newly assigned as authorized users or newly hired after AVST equipment is in operation have 30 days from their hire date or being assigned the job duty to complete the training. The training should be assigned and completed at least every two years or when a new/updated version is available. The AVST committee may elect to designate a committee member to periodically or routinely verify if the required training has been completed.

Complaints and Questions Regarding AVST

Complaints or questions about the installation or use of AVST equipment may be directed to the AVST committee in writing by email to avst@tamu.edu. The committee will review the issue at hand and respond to the requestor as appropriate; formal complaints will be follow standard processes as outlined in related university rules and standard administrative procedure.