

# Texas A&M University System Standard – Security Surveillance

## Standard Statement

---

This standard establishes transparent processes and controls for using audiovisual surveillance equipment and any resulting recorded material.

---

## Definitions

---

Audiovisual Surveillance: Cameras or similar technology used to enhance security, safety, and quality of life for the System Office.

AVST: Audiovisual surveillance technology.

Active AVST Installation: Cameras or similar technology that are viewing/recording activities within the area of surveillance.

---

## Official Standard

---

### 1. General

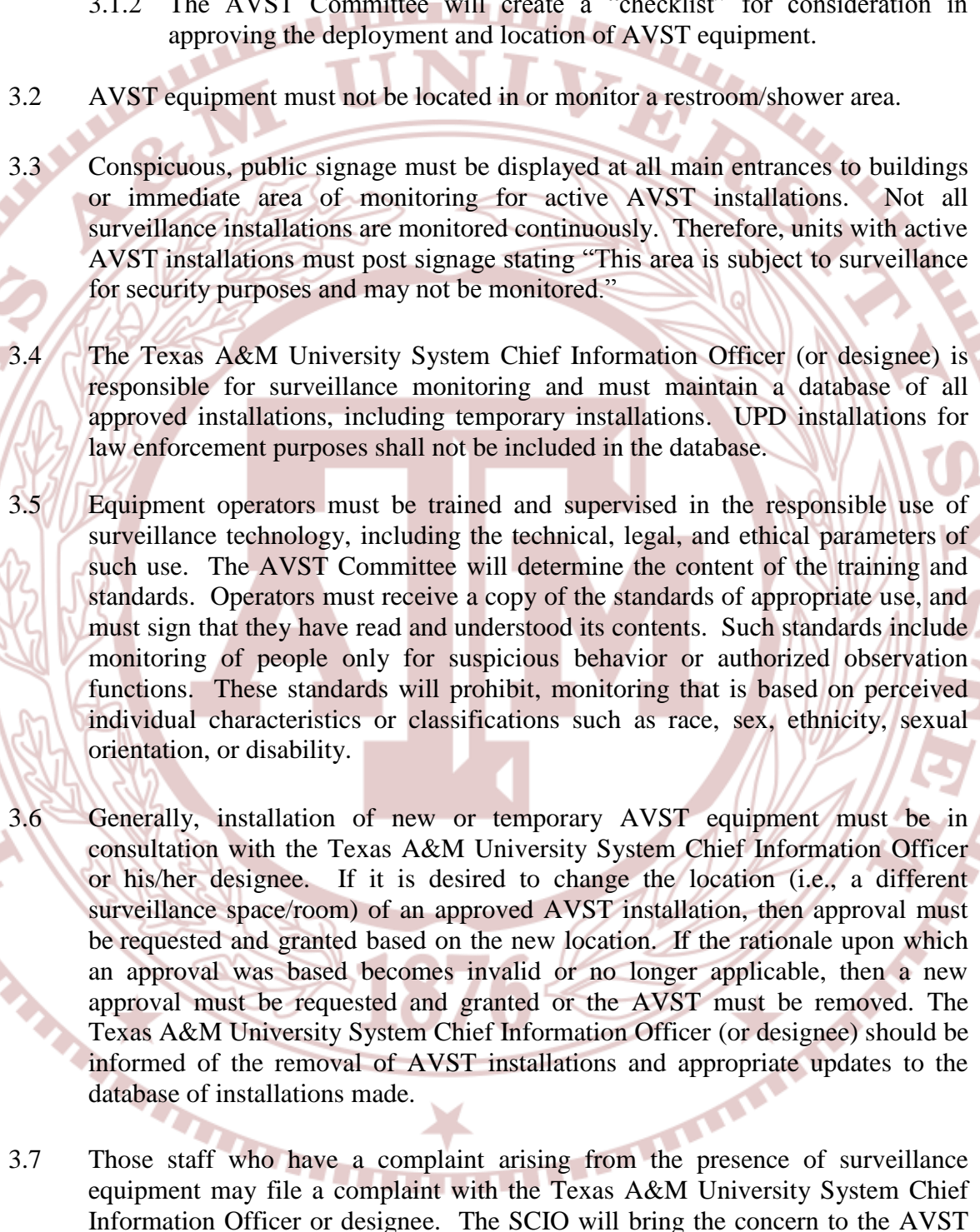
The System Office (SO) strives to provide a secure environment for members of its community and to protect state property. Ensuring a secure environment can be assisted by audiovisual surveillance technology. Such technologies must be used responsibly and within the intended scope of the purpose for their deployment.

### 2. Applicability

All installations of audiovisual surveillance technology must comply with these standards except those installations authorized by the University Police Department (UPD) or System Internal Audit.

### 3. Standards

3.1 An Audiovisual Surveillance Technology (AVST) Committee shall be established by the Texas A&M University System Chief Information Officer to review AVST installations for appropriateness, to verify consistent application of surveillance controls, and to review complaints regarding the use or placement of AVST. The AVST Committee shall be composed of representatives of the SO community including, but not limited to, TAMUS CIO, TAMU Networking and Information Security, University Police Department (UPD), Human Resources, Office of General Counsel (OGC).

- 
- 3.1.1 The purpose of the AVST Committee is to provide recommendations to the TAMUS CIO (or designee) regarding the use of AVST.
- 3.1.2 The AVST Committee will create a “checklist” for consideration in approving the deployment and location of AVST equipment.
- 3.2 AVST equipment must not be located in or monitor a restroom/shower area.
- 3.3 Conspicuous, public signage must be displayed at all main entrances to buildings or immediate area of monitoring for active AVST installations. Not all surveillance installations are monitored continuously. Therefore, units with active AVST installations must post signage stating “This area is subject to surveillance for security purposes and may not be monitored.”
- 3.4 The Texas A&M University System Chief Information Officer (or designee) is responsible for surveillance monitoring and must maintain a database of all approved installations, including temporary installations. UPD installations for law enforcement purposes shall not be included in the database.
- 3.5 Equipment operators must be trained and supervised in the responsible use of surveillance technology, including the technical, legal, and ethical parameters of such use. The AVST Committee will determine the content of the training and standards. Operators must receive a copy of the standards of appropriate use, and must sign that they have read and understood its contents. Such standards include monitoring of people only for suspicious behavior or authorized observation functions. These standards will prohibit, monitoring that is based on perceived individual characteristics or classifications such as race, sex, ethnicity, sexual orientation, or disability.
- 3.6 Generally, installation of new or temporary AVST equipment must be in consultation with the Texas A&M University System Chief Information Officer or his/her designee. If it is desired to change the location (i.e., a different surveillance space/room) of an approved AVST installation, then approval must be requested and granted based on the new location. If the rationale upon which an approval was based becomes invalid or no longer applicable, then a new approval must be requested and granted or the AVST must be removed. The Texas A&M University System Chief Information Officer (or designee) should be informed of the removal of AVST installations and appropriate updates to the database of installations made.
- 3.7 Those staff who have a complaint arising from the presence of surveillance equipment may file a complaint with the Texas A&M University System Chief Information Officer or designee. The SCIO will bring the concern to the AVST Committee for disposition.

- 3.8 Units administering AVST equipment must design monitoring locations to prevent tampering with recorded material. Cameras and similar technologies must have sufficient security measures (e.g., encryption) to prevent unauthorized access to the output of the equipment. Access must require authentication over a secure channel (e.g., SSL). Video output need not be encrypted, but reasonable measures should be taken to mitigate interception as approved by the AVST. Web cameras intended for general access to public events must be approved in advance, and privacy concerns must be specifically addressed in the request.
- 3.9 Recorded surveillance material shall be stored in secure locations accessible only to designated individuals. Such records are deemed “Transitory Information” and shall be retained for no less than fourteen (14) days and no longer than 31 days. Records preserved for longer than 31 days relevant to a specific official investigation 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 Texas A&M University System Chief Information Officer or designee. Documented retention periods for existing equipment that cannot meet this requirement must be submitted to the Texas A&M University System Chief Information Officer or designee.
- 3.10 Requests for the review/release of recorded AVST data/recordings must be reviewed and approved by the information resource owner (or designee) unless release is required by State or Federal law.
- 3.11 AVST data/recordings will be treated as confidential with regard to internal System Office procedures. The data/recordings may only be released for review as a result of normal procedures and regulations for the release or disclosure of information such as investigations by authorized System Office officials, subpoenas/court orders, or Public Information Requests. Requests and any needed approvals for the review/release of data/recordings shall be fully documented.

---

### Contact Office

---

For clarification or interpretation, contact Texas A&M University System Chief Information Officer.

**OFFICE OF RESPONSIBILITY:** Texas A&M University System Chief Information Officer