I. 8.7.2 Security

Chapter 8 - Health & Safety	Original Effective Date: June 2000
Section: 8.7 University Policy	Date Last Reviewed: December 2024
Responsible Entity: Chief, University Police	Date Last Revised: December 2024

II. Purpose

To establish and maintain a set of minimum security standards for all buildings with alarms and cameras requiring a response from the UT Police Department (UTPD) and to develop a standard of consistent guidelines regarding the purchase, installation, and operation of alarm systems on campus to be used by UT Health San Antonio (University) departments or any non-university entity under contract with the University. This Policy also relates to the use of video recording and closed-circuit television (CCTV) security systems in maintaining safety and security while preserving privacy rights of the University community and the public, in accordance with all applicable laws and policies.

III. Scope

This Policy applies to all departments, employees, and students with respect to the installation and use of access controls, alarms, video, IP, security, and CCTV cameras in facilities owned or controlled by the University, except as noted below. All references to video cameras throughout this Policy are for those systems which were designed and installed with the intent and ability to record video and/or to be monitored live. This Policy governs all new and existing departmental video camera monitoring systems.

A. This Policy does not apply to:

1. Use of video recording and CCTV technology covered by University policies governing research with human subjects or animals.
2. Use of video recording and CCTV technology for video conferencing.
3. Use of class lecture recordings and/or archiving for the purpose of content sharing.
4. Use of mobile video/audio recording systems used by the UTPD.
5. Use of cameras in the UTPD Temporary Detention and Interview Rooms.
6. Use of body worn cameras used by the UTPD.

8.7.2 Security

IV. Policy

The goal of minimum building security standards is to ensure that the deployment of new security devices is done uniformly in all like spaces and provides a tool for planning and design of new security systems installation so that occupants and UTPD, as first responders, will have the most effective tools for protecting personal safety and against property theft. Therefore, any new construction or renovation projects will adhere to the minimum building security standards as approved by the Chief of Police. In buildings where existing security is below minimum standards, the goal is to make improvements towards the standards over time and as budgets allow.

A. Buildings

Buildings will be secured after normal business hours, weekends, and holidays.

B. After-Hour Entry

Doors fitted with access control card readers may be used for entry to buildings after normal business hours. The UTPD communications personnel may upon request permit entry into the building after receiving proper identification and authorization. ID verification and patron status is required for entry.

C. Access Control

1. An Access Control device is a card reader or card reader with a keypad combination with alarm signals and/or maintenance signals that report to the UTPD for monitoring.
2. To ensure that all doors and related hardware will work with the existing security/access control system, the Chief of Police is responsible for approving all new software, hardware, card readers, etc. related to access control.
3. The UTPD is responsible for programming and/or reprogramming all electronic access systems.
4. All access control hardware must be purchased or acquired from the vendor specified by UTPD.

D. Alarms

All costs for the purchase and installation of security system alarm devices shall be borne by the appropriate project budget or the department or unit making the requests, with the understanding that meeting the minimum standards is the goal.

Failure to comply with operating procedures, as set forth herein, or in an operation manual or failure to comply with the stipulations of this Policy may result in the system being disconnected or discontinued from operation

1. Security Alarm Installation

   Departments and non-university entities located on campus may desire to install security alarm systems where assets and/or sensitive property are of sufficient value

to warrant protection. A request form for the installation or expansion of an alarm system, to be monitored and responded to by the UTPD personnel, must be submitted and approved by the Chief of Police or designee.

2. Security Alarm Compatibility

   Any security alarm system installed must be compatible with and connected to the standard monitoring equipment used by UTPD, unless otherwise approved by the Chief of Police or designee.

3. Response Process

   The UTPD will develop a response process for each installed alarm system.

4. Periodic Security Alarm Inspection

   It is the responsibility of the Access Control Manager to inspect alarms periodically and to immediately report malfunctions to Facilities Management for repairs.

5. Security Alarm Activity List

   The UTPD Access Control Manager is responsible for updating and maintaining a current list of active alarms on campus.

6. Hold-up or Panic Buttons

   A justified written request for the installation of hold-up/panic button must be submitted to the Chief of Police for approval.

E. Security Cameras

When deploying CCTV and/or video security systems on campus, the System Manager and all individuals granted access to those systems are required to abide by the responsibilities and procedures set forth in this Policy.

1. Purpose for Use of Monitoring Systems

   The purpose of video and CCTV monitoring governed by this Policy is for enhanced safety and security for the university community. Any interception, duplication, transmission, or other diversion of video and CCTV technologies for purposes other than the safety and security contemplated by this Policy is prohibited. Safety and security purposes include, but are not limited to:

   a. Protection of individuals, including students, faculty, staff, and visitors.
   b. Protection of University owned and/or operated property and buildings, including building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, and cashier locations.
   c. Monitoring of common areas and areas accessible to the public, including transit stops, parking lots, parking garages, elevators, public streets, and pedestrian walks.
   d. Investigation of criminal activity.
   e. Protection against an act of terrorism or related criminal activity.

f. Protection of Critical Infrastructure as defined under the Texas Homeland Security Act, the USA Patriot Act, or the United States Department of Homeland Security.

2. Monitoring System Protocol
    a. Video and CCTV monitoring and recording are required to be conducted in accordance with all existing University policies.
    b. Monitoring or recording of audio is strictly prohibited.
    c. Monitoring shall be limited to uses that do not violate a reasonable expectation of privacy.
    d. Cameras may be monitored in real time, but cameras may also be unmonitored while recording.
3. Monitoring System Usage Requirements
    a. Signage for video and CCTV locations may be installed at main entrances to areas with video security, such as building entrances and elevator landing areas.
    b. All future and existing departmental video/CCTV monitoring systems governed by this Policy are required to comply with this Policy including technical specifications for both IP and CCTV cameras.
    c. The System Manager is authorized to oversee the use and installation of CCTV monitoring for safety and security purposes at the University.
    d. The Chief of Police, or designee, may authorize any temporary camera installation, as deemed necessary in connection with a criminal investigation, for enhanced security for special events, or as otherwise deemed necessary to enhance safety and security at the University. Temporary cameras must be removed once investigations are concluded.
    e. All operators and supervisors involved in video surveillance are required to perform their duties in accordance with this Policy.
    f. All departments with access to a video/CCTV monitoring system governed by this Policy are required to perform their duties in accordance with this Policy.
    g. Personnel involved in monitoring and recording must be trained and supervised by their department in the responsible use of the technology and the requirements of this Policy.
4. All Camera Control Operators
    a. Must be trained in the technical, legal, and ethical parameters of appropriate camera use. Training is to cover the proper operation and maintenance of department's equipment and infrastructure.
    b. Must not monitor individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other classifications protected by the University's Non-Discrimination Policy. (See Institutional Handbook of

Operating Policies (IHOP) Section 4.2.1 Nondiscrimination Policy And Complaint Procedure.)

c. Must not view places where people have a right to privacy, including but not limited to bathrooms, dressing rooms, locker rooms, or private rooms.

d. The System Manager is required to review the Policy, implementation guidelines, and equipment specifications as necessary to comply with the Policy and must make recommendations for changes.

5. Records Retention

a. Recordings must be retained for a period not to exceed 31 days, or for periods not to exceed 60 days for certain labs. After those time periods, recordings are required to be erased, or recorded over, unless retained as part of a criminal investigation or court proceeding (either civil or criminal) or other authorized use as approved by the Chief of Police, after consultation with the Office of Legal Affairs.

b. Recordings must be retained in a secure location with access by authorized personnel only.

6. Requests for Information Obtained from Monitoring Systems

a. Information relating to ongoing criminal investigations and anti-terrorism must only be released when approved by the Chief of Police or designee after consultation with the Office of Legal Affairs.

b. Open Records Requests for recorded video must be forwarded to the Open Records Officer.

c. Lawful requests (e.g., subpoenas, search warrants) for recorded video must be forwarded to the Office of Legal Affairs.

d. The Office of Legal Affairs is responsible for reviewing and responding to all subpoenas from law enforcement to release recordings obtained through Video and CCTV monitoring.

7. Request for Cameras

a. Departments are to make requests to the System Manager for the installation of cameras.

b. The System Manager will meet with the requesting department and conduct a site visit.

c. The System Manager will provide the department a cost estimate for the installation.

d. Departments are responsible for all costs associated with the installation of cameras.

i. All camera installations must be approved by the Chief of Police, or designee.

8.7.2 Security

V. Definitions

When used in this document, the following words have the meaning set forth below unless the context requires a different meaning.

Closed-Circuit television (CCTV) – the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. CCTV systems may operate continuously or only as required to monitor a particular event. CCTV video used for security purposes pursuant to this policy must always be restricted to a secure private network or Virtual Private Network (VPN) which may only be accessed by authorized persons

Internet Protocol (IP) Cameras – cameras which use the protocol used most by Local Area Networks (LANs) to transmit video across data networks in digital form. IP video used for security purposes pursuant to this policy must always be restricted to a secure private network or VPN which may only be accessed by authorized persons.

System Manager– the individual who is responsible for the management of a University video recording and/or CCTV system as governed by this Policy.

Video Cameras – includes all analog and digital cameras whether wired or wireless.

Video Monitoring – real time monitoring of security video of an event that is in progress is to enhance the safety and security of the event.

Video Security System – video recording systems installed for the purpose of prevention against assault, damage, theft, unlawful entry, and other such occurrences caused by deliberate actions.

Video Surveillance – ongoing close observation and collection of data or evidence for a specified purpose or confined to a narrow sector. This can include real time video monitoring or automated recording.

VI. Related References

There are no related documents associated with this Policy.

VII. Review and Approval History

The approving authority of this policy is the University Executive Committee.

Effective Date	Action Taken	Approved By	Approved Date
06/2000	Policy Origination		
02/2016	Policy Revision		
08/2021	Policy Revision/Discretionary Edit	UTPD	
12/2024	Policy Revision/Discretionary Edit	UTPD	12/17/2024