Utah Tech University Policy

465: Video Surveillance

I. Purpose

1.1 Utah Tech University ("the University") regulates and authorizes Video Surveillance on University Premises in a professional, ethical, and legal manner in order to enhance public safety and security for the University Community to ensure academic integrity, operational effectiveness, and compliance with University policy. This policy regulates all Video Surveillance on University Premises.

II. Scope

2.1 Use or installation of Camera or video equipment by any University Community Member, department, or entity for the express or implied purpose of surveillance is subject to this policy. Use or installation of video or Camera equipment for purposes other than surveillance is not subject to this policy. Non-surveillance purposes include, but are not limited to, academic instruction, research, video conferencing, recording and/or transmission of public events or performances, use of web and mobile phone cameras, etc.

III. Definitions

3.1 ***Camera:*** Any digital or analog device that can capture or transmit visual images designed to monitor a specific area, including but not limited to video Cameras, still Cameras, cellular telephones, webcams, electronic surveillance systems, and computing devices.

3.2 ***Content:*** All information, whether audio or video, captured by University public safety camera systems. This includes system logs, stills, snapshots, stop action, and video images whether transient, displayed, or recorded.

3.3 ***Private Spaces:*** Areas in which individuals have a reasonable expectation

of privacy, including but not limited to restrooms, locker and dressing rooms, and individual residential rooms.

3.4 ***University Community Member:*** An individual employed by or affiliated with the University or a participant in any University program or activity, including but not limited to, administrators, faculty, staff, students, independent contractors, volunteers, trustees, advisory board members, and guests or visitors to any University Premises.

3.5 ***University Premises:*** All land, buildings, facilities, and other property in the possession of, or owned, used, leased, or controlled by the University.

3.6 ***Video Surveillance:*** Viewing, recording, or making available for viewing visual images of University Premises in the form of photographs, video recordings, live feeds, or in other formats.

3.7 ***Video Surveillance System:*** All components of Video Surveillance including hardware, software, Camera installations, recording protocol, monitoring, etc.

IV. Policy

4.1 All non-private areas of the University Premises are subject to Video Surveillance for the purposes defined by this policy. Except as directed by lawful court order, Video Surveillance cameras will not be directed at private spaces on or off University Premises.

4.2 Collecting or recording audio Content as part of Video Surveillance is specifically prohibited unless it is part of Video Surveillance excluded from this policy or is undertaken as the result of court order issued lawfully under state or federal law or regulations.

4.2.1 An exception to this policy is The Testing Center's independent audio and video content surveillance systems that provide third-party vendors with remote access to ensure exam integrity.

4.3 The University operates a central Video Surveillance System to manage all Video Surveillance installations and centralize viewing and recording of video feeds. This System and its uses are authorized and controlled by the Vice President of Administrative Affairs.

4.3.1 The University's Police Department ("UTPD") and Information Technology Services ("IT") operate the central Video Surveillance System under the direction of the Vice President of Administrative Affairs, and maintain standards and guidelines, governed by this policy, regarding use and operation of the University Video

Surveillance System.

4.3.2 University departments may fund specific Video Surveillance installations in areas of the University under their control or interest, but departments may not install or operate these Video Surveillance installations. Unless otherwise arranged with the Vice President of Administrative Affairs, departments retain ongoing fiscal responsibility for maintenance of such installations.

4.3.3 IT maintains site installation standards and is responsible for installation and technical maintenance of all Video Surveillance Systems.

4.3.4 No other Video Surveillance may be installed on University Premises without prior written approval of the Vice President of Administrative Affairs.

4.4 Purpose and approved usage of Video Surveillance: The following are approved uses of, and approved purposes for, Video Surveillance:

4.4.1 When conducted by UTPD or another law enforcement agency to deter, detect, or investigate actual or alleged criminal activity, to directly prevent harm or a threat to public safety, or to protect University resources and property of University Community Members from loss or damage.

4.4.2 When reviewed by an appropriate University official as part of an administrative investigation involving Academic Integrity, Academic or Professional Misconduct, or operational effectiveness under University conduct and other applicable policies. The Office of General Counsel must preapprove access to Video Surveillance Content by a non-UTPD official for any administrative investigation in which discipline or sanctions of suspension, dismissal, or termination of a student or employee may result.

4.4.2.1 To support the University's academic mission, the Testing Center and third-party testing partners may review and export video and audio content related to Academic Misconduct to the Dean of Students and University faculty, as necessary (See Policy 555).

4.4.3 Other operational effectiveness purposes approved by the applicable University Vice President: Examples include, but are not limited to, monitoring of lobbies and reception areas, monitoring and review of sales floors and cashiering areas, and monitoring of

University special events. These purposes must be explicitly approved by the applicable University Vice President.

4.4.4 Collecting or using of Video Surveillance must be in accordance with the Family Educational Rights and Privacy Act (FERPA) and other applicable state and federal law and regulations. Video Surveillance Systems and/or Content may not be collected or used to target, reconnoiter, or otherwise unduly monitor a specific individual(s) based on race, sex, ethnicity, nationality, gender, disability, religion, or other protected class.

4.5 Access to Video Surveillance Systems: UTPD and IT personnel authorized by the Vice President of Administrative Affairs shall have access to all live and recorded surveillance feeds directly related to the performance of their duties to provide public safety and security, protect University assets, and to operate and maintain the University Surveillance System.

4.5.1 Appropriate University officials with a need-to-know purpose in accordance with the uses noted above in Section 4.4.2 and with the preapproval of the Office of General Counsel may coordinate with UTPD to review and/or export Surveillance Content.

4.5.2 Persistent access to the Surveillance System for other employees to view live Video Surveillance feeds must be preapproved by the applicable University Vice President. Such persistent access to surveillance feeds must be based on an employee's need-to-know basis and in harmony with the purposes for Video Surveillance as stated in this policy. Access procedures will be maintained by UTPD and IT.

4.5.3 The UTPD is authorized to export recorded Video Surveillance Content or feeds from the Video Surveillance System. Other employees may be authorized to export recorded Video Surveillance Content on a case-by-case basis approved by the Vice President of Administrative Affairs when an appropriate academic or business purpose exists. All other requests to view and/or export recorded Content must be requested from UTPD.

4.5.4 An ad-hoc review committee, chaired by the Vice President of Administrative Affairs, or Designee, and including representatives from the University Safety and Risk Management Department and IT, shall meet no less than biennially. This committee will review access privileges for all employees using the University Surveillance system to ensure that each employee's access is appropriate to that employee's role and in harmony with the purposes of Video

Surveillance as stated in this policy. This committee may adjust or revoke Video Surveillance privileges.

4.6 Release of Video Surveillance Content: No University employee is authorized to publicly release or provide Video Surveillance footage under any circumstances unless the following criteria exist:

4.6.1 Release is made by UTPD in consultation with the Office of General Counsel to comply with a court order, search warrant, subpoena, or law enforcement request issued lawfully under federal or state law or regulation.

4.6.2 Release is required in response to a public record request and is approved solely by the Office of General Counsel.

4.6.3 Release is approved by the University President or the Vice President of Administrative Affairs after consultation with the UTPD Chief of Police and the Office of General Counsel.

4.7 Written Request for Change of Location or Visual Range

4.7.1 Any member of the University Community may submit a written request to the Vice President of Administrative Affairs to change the location or limit the visual range of Video Surveillance equipment based on a belief that the location or the visual range of the equipment infringes on that individual's reasonable expectation of privacy or protected rights.

4.7.2 Specific information regarding the location or the visual range, the right believed to have been infringed, and how the installation infringes on that right must be included in the written request.

4.7.3 The Vice President of Administrative Affairs, or Designee will, after consultation with UTPD, respond to the request within thirty (30) University Business Days of receipt. The response from the Vice President of Administrative Affairs, or Designee, may not be appealed.

4.8 Retention

4.8.1 Surveillance Content must be stored in a secure location and configured to prevent their unauthorized access, modification, duplication, or destruction.

4.8.2 Surveillance Content will be retained for at least fourteen (14) days or more. Therefore, all surveillance installations must be capable of

retaining Content for at least this period of time.

4.8.3 After the fourteen (14) day retention period, the content may be erased, or recorded over, unless retained as part of a criminal investigation, court proceeding, or other authorized use as approved by the Vice President for Administrative Affairs, or as required by state or federal law or regulations.

4.8.4 For uses not listed in section 4.4 of this policy, UTPD shall maintain for a period of twelve (12) months from the date of access a log documenting all access by non-UTPD and non-IT personnel to Content derived from the University's centralized Video Surveillance System.

4.8.5 An individual member of the University Community who seeks to access and use Video Surveillance Content from the University for purposes of conducting academic research will ordinarily be required to submit a request through the GRAMA process for obtaining University records. The request will be subject to the same restrictions and requirements as a request made by a non-University party. Additionally, any use of such Video Surveillance Content involving research with human subjects is subject to legal and University requirements for such research, including preapproval by the University's Institutional Review Board before any data is collected.

4.8.6 University personnel who misuse Video Surveillance Content or facilitate the misuse of Video Surveillance Content by another person are subject to discipline under applicable University Policy. Such misuse may also be subject to criminal penalties or civil liability under applicable law. The University may audit any Video Surveillance System at any time to detect improper system operation or misuse of Content.

V. References

5.1 Code of Federal Regulations Title 45 HHS Part 46, Protection of Human Subjects https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html

5.2 Family Educational Rights and Privacy Act (FERPA)

5.3 Government Records Access and Management Act (GRAMA)

5.4 University Policy 555: Student Academic and Professional Misconduct

5.5 University Policy 607: Institutional Review Board (IRB)

VI. Procedures—N/A

VII. Addenda – N/A

Policy Owner: Vice President of Administrative Affairs
Policy Steward: Chief Information Officer; Information Security Officer

History:
Approved 4/29/16
Revised 11/12/21
Editorial 07/01/22
Revised 11/11/22