

Oregon Tech Policy OIT-30-008 Security Cameras

1. Policy Statement

Oregon Tech deploys security cameras on its campuses to advance legitimate public safety and security interests, including, without limitation:

- Safeguarding of human life.
- Protection of buildings owned, occupied, or controlled by the university.
- Investigation of criminal activity.
- Investigation of alleged misconduct, whether or not rising to the level of a criminal offense.
- Monitoring access to university controlled facilities.
- Verifying fire, life safety and security alarms.
- Rapidly responding to emergencies.
- Maintaining situational awareness of campus activities and events.

The primary purpose of Oregon Tech's security cameras is to enhance the safety and security of the campus community while recognizing and preserving individual privacy and freedom of expression.

As set forth in this policy, the university will ensure that security cameras are used in a professional, ethical, and legal manner in accordance with this and other relevant university policies, as well as applicable federal and state laws.

2. Reason for Policy/Purpose

The purpose of this policy is to create a governance and management framework that will guide the university in the use of security cameras, across the organization.

3. Applicability/Scope

This policy applies to all Oregon Tech security camera systems.

4. Definitions

Authorized User: Any Oregon Tech affiliated individual authorized by the Security Technology Administrator to have ongoing viewing access to security camera data and recordings.

Private Space: Any space in which an individual has a reasonable expectation of privacy, including but not limited to residential living areas, bathrooms, shower areas, locker and changing rooms, lactation rooms, and rooms used for medical, physical, or mental health treatment.

Public Space: Any space not defined as a private space, including but not limited to campus grounds, parking areas, building exteriors, loading docks, areas of ingress and egress, classrooms, lecture halls, study rooms, lobbies, theaters, libraries, dining areas, gymnasiums, recreation areas and retail establishments.

Security Camera: a camera used for safety and security purposes, which are enabled only to make visual recordings (i.e., no audio recordings).

Security Camera System: any electronic service, software or hardware directly supporting or deploying security cameras.

Security Camera Data/Recordings: any analog or digital video data captured by security cameras that can be monitored, transmitted, stored, retrieved, or modified.

Security Technology Administrator: the Executive Director for Resilience, Emergency Management and Safety shall serve as the Security Technology Administrator responsible for the installation, management, operation, maintenance, and use of the infrastructure associated with security technology. Further, the Security Technology Administrator is responsible for data access and maintenance. Assistant Security Technology Administrators may be designated as appropriate.

5. Policy Details

5.1 Exclusions

This policy does not apply to:

- Use of cameras for the delivery of education in the classroom, lab, or similar setting, including remote learning and assessment of performance-based learning activities.
- Use of cameras for research, as defined under federal law and governed by university policy involving human subjects or animals.
- Use of cameras to record public performances, events, or interviews, or when permitted on campus for broadcast purposes in accordance with university procedures governing filming on-campus.
- Use of cameras for business purposes such as video conferencing.
- Use of cameras for the purpose of providing accommodations for persons with disabilities.
- Use of publicly accessible web-cameras with no recording capability for routine use by the university.
- Use of body worn or mobile cameras by Campus Safety.
- Use of concealed surveillance cameras in connection with criminal investigations.
- Use of cameras for licensed banking operations on university property which are conducted in accordance with state and federal regulations.
- Use of cameras utilized by non-university personnel.

5.2 Oversight

The Security Technology Coordinating Committee (the Committee) includes an interdisciplinary team of stakeholders charged with governing the use of security technology (e.g., access control, panic alarms, security cameras, video intercom systems, etc.), excluding cybersecurity technology, throughout the university.

The Committee will be responsible for assessing and approving any requests to acquire, install, modify, and/or decommission university security technology. In addition, the Committee will oversee the development and implementation of policies and procedures relating to the acceptable use of security technology.

The Committee reports to the Vice President for Finance and Administration, and is chaired by the Security Technology Administrator (Executive Director for Resilience, Emergency Management and Safety). Membership includes representatives from Campus Safety, Facilities Services, Human Resources, Information and Technology Services and Student Affairs.

5.2.1 Security Camera Installation

The installation of new security cameras must be approved in advance by the Security Technology Coordinating Committee and the Vice President for Finance and Administration.

Request for new security cameras must be based upon evidence of a need to mitigate an identified safety and security risk or vulnerability.

Once approved, new security cameras shall be fully integrated into the university-wide security camera system. Independent or standalone security cameras and/or systems are not permitted.

5.2.2 Security Camera Placement

The placement of security cameras shall be in accordance with this policy and limited to uses that do not violate the reasonable expectation of privacy as defined by law. University security cameras will not be placed within private spaces. Additionally, university security cameras will not be placed within faculty and staff offices.

5.2.3 Public Notice

Signs shall be posted in a conspicuous manner, strategically located in plain view, notifying individuals that activity is being recorded by a university security camera system.

The following language is required on all signs:

This area is recorded 24 hours per day by a university security camera system. For questions, please contact Oregon Tech Campus Safety at 541-885-1111.

5.2.4 Monitoring of Security Cameras

Neither the installation of security cameras nor this policy constitutes an undertaking by the university to provide continuous live monitoring of all locations visible through such security cameras. Security cameras may be monitored in “real time” by trained personnel when safety or security concerns, event monitoring, ongoing investigations, alarms, or other situations warrant such monitoring. The monitoring of activities of individuals or groups shall be conducted in a manner consistent with this policy and applicable legal requirements.

5.2.5 Access to Security Camera Data or Recordings

Only the Security Technology Administrator or trained Authorized Users will be involved in, or have access to, stored security camera data or recordings. Security cameras will be installed and configured to prevent tampering with or unauthorized duplication of data and recordings.

5.2.6 Retention of Security Camera Data or Recordings

Security camera data or recordings will be stored for a period generally not to exceed 90 days and thereafter will be erased, unless the recording is subject to a valid court or agency preservation order or a university litigation hold, retained as part of an active investigation, released and used for the purposes described below, or needed for legitimate training or other purposes, as may be determined by the Executive Director for Resilience, Emergency Management and Safety or the General Counsel. Data or recordings will be stored in a secure environment accessible to authorized personnel only, and will not be reviewed absent a legitimate institutional purpose.

5.2.7 Release of Security Camera Data or Recordings

Relevant portions of security camera data and recordings may be released by the Executive Director for Resilience, Emergency Management and Safety as follows, upon request:

- Vice President for Student Affairs, the Dean of Students, or their designees in connection with an investigation or adjudication of an alleged violation of the Student Code of Conduct.
- Associate Vice President for Human Resources and senior university administrators in connection with an investigation of alleged workplace misconduct.
- Executive Director for Diversity, Inclusion and Cultural Engagement/Title IX Coordinator, Title IX Deputy Coordinators, or external contracted investigators in connection with an investigation or adjudication of allegations related to equity, sexual misconduct, harassment, and Title IX.
- Senior university administrators to assist in the assessment of and response to actual or threatened criminal or nefarious activity, a pattern of recurring disturbances to the university community, a legitimate safety concern or campus emergency.
- Security camera data or recordings may not be used to evaluate job performance of Oregon Tech faculty and staff, except as related to workplace misconduct as described above or prohibited by Oregon Tech policy.

All other requests or demands for access to security camera data or recordings, including requests under the Oregon Public Records Law and all subpoenas, warrants, court orders and other legal

documents directing access to law enforcement agencies or others must be conveyed to the Public Records Officer within the Office of the General Counsel.

Nothing in this policy shall be deemed to restrict the use of security camera data or recordings by the university in the defense of actual or threatened claims, legal actions or other proceedings brought against it or the disclosure to appropriate university administrators who are directly involved in responding to such claim, actions, or proceedings.

5.2.8 Procedures

Campus Safety will maintain written procedures relating to the use of security camera technology. These procedures shall be reviewed and agreed upon by the Security Technology Coordinating Committee prior to implementation.

5.2.9 Training

All security camera Authorized Users must receive annual training on technical, legal, and ethical use of security cameras and data retention and release. Training shall include a review of all procedures and this policy.

5.2.10 Compliance

Any violation of this policy or associated procedures may be considered misconduct resulting in removal of security cameras, denial of access to security camera data and recordings, and if applicable, corrective, or disciplinary action, up to and including termination.

5.2.11 Existing Security Camera Systems

Security camera systems that predate the effective date of this policy shall be brought into compliance with this policy within six (6) months of the effective date of this policy. Unapproved or nonconforming security camera systems may be removed by the Security Technology Coordinating Committee with the approval of the Vice President for Finance and Administration.

5.2.12 Review

The Security Technology Coordinating Committee shall review this policy, associated procedures and mandatory Authorized User training on an annual basis.

6. Links to Related Procedures, Forms, or Information

<https://www.oit.edu/remc>

<https://www.oit.edu/public-records>

7. Policy Review/Consultation

This policy was reviewed and open to consultation by the following Oregon Tech committees

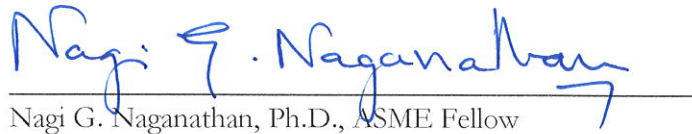
and/or advisory groups:

- Faculty Senate

This policy was revised pursuant to Oregon Tech's policy review and making process.

8. Policy Approval

Approved by the President on January 7, 2025.

A handwritten signature in blue ink that reads "Nagi G. Naganathan". The signature is written in a cursive style and is positioned above a horizontal line.

Nagi G. Naganathan, Ph.D., ASME Fellow
President

Adoption Date

July 31, 2024

Supersedes

OIT-30-008 dated July 31, 2024

Revision Dates

December 3, 2024