# Oregon Tech Policy OIT-30-008 SECURITY CAMERAS-INTERIM

## 1. Policy Statement

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

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

**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 camera.

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

Policy Details

#### a. Exclusions

This policy does not apply to:

- š 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;
- š Use of cameras for research, as defined under federal law and governed by university policy involving human subjects or animals;
- S 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;
- š Use of cameras for business purposes such as video conferencing.
- š Use of cameras for the purpose of providing accommodations for persons with disabilities.
- š Use of publicly accessible web-cameras with no recording capability for routine use by the university;
- š Use of body worn or mobile cameras by Campus Safety;
- š Use of concealed surveillance cameras in connection with criminal investigations.
- š Use of cameras for licensed banking operations on university property which are conducted in accordance with state and federal regulations; or
- š Use of cameras utilized by non-university personnel.

#### b. 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,

2 – Security Cameras Version date: 08/01/24

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

3 – Security Cameras Version date: 08/01/24

All security camera Authorized User 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.

## I. 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

## m. 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.

#### n. 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/rems

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

## 7. Policy Review/ Consultation

This Policy was approved on an interim basis by Oregon Tech's President pursuant to Board Policy on Delegation of Authority, Section 2.3. The Policy will be presented to the President's Council for review when the body reconvenes in Fall 2024.

Version date: 08/01/24

#### 8. Policy Approval

Approved by the President on July 31, 2024.

DocuSigned by:

Masi Massinathan

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

President

5 – Security Cameras