BOISE STATE UNIVERSITY

University Policy 12140

Public Safety Camera Systems

Effective Date

September 2015

Revision Date

July 2019

Responsible Party

Department of Public Safety, (208) 426-6911

Scope and Audience

This policy applies to all faculty, staff, students, and campus units within the University. This policy does not apply to content used for research with human subjects, animals, classroom capture, or video conferencing.

Additional Authority

- University Policy 1060 (Non-discrimination and Anti-harassment)
- University Policy 1020 (University Records, Archives and Publications)
- University Policy 1030 (Litigation Hold)
- University Policy 1040 (Public Records)
- University Policy 1065 (Sexual Harassment, Sexual Misconduct, Dating Violence, etc…)

1. Policy Purpose

To regulate and centralize the use of Public Safety Camera Systems used to observe and record public and Personal Areas.

2. Policy Statement

Boise State University is committed to providing a safe and secure campus while safeguarding the privacy of University students, faculty, staff, community partners, and visitors. The primary use of Public Safety Cameras is to record video images for use by law enforcement, the Department of Public Safety, and other University officials charged with investigating alleged violations of University policy. Any interception, duplication, transmission, or other diversion of Content for purposes other than what is authorized by this policy is prohibited. The existence of this policy does not imply or guarantee security cameras will be monitored in real time continuously or otherwise.

Lecture capture systems, video conferences, and video recording of test subjects in research situations, as well as other academic/research-related recordings, are generally exempt from this policy.

3. Definitions

3.1 Camera Control Managers

Individuals designated by campus units who are responsible for a unit's recording, reviewing, and recovering of Content.

3.2 Content

All information, whether audio or video, captured by a Public Safety Camera System. This includes system logs, stills, snapshots, stop action, and video images whether transient, displayed, or recorded.

3.3 Personal Areas

A location where a reasonable person would expect privacy such as residence hall living quarters, public restrooms, locker rooms, or other areas as defined by law.

3.4 Public Safety Camera Systems

A fixed or moveable camera used for monitoring or recording public and Personal Areas for the purposes of enhancing public safety, discouraging theft and other criminal activities, monitoring ingress and egress, and investigating University policy violations. It includes the camera's Content and any physical spaces, electronic service, software, or hardware directly supporting or deploying the camera.

4. Responsibilities and Procedures

4.1 Integrated Security Technology Committee (ISTC)

a. The ISTC is responsible for creating and monitoring protocols for the storage and retention of Content as well as developing procedures to regularly assess and review existing Public Safety Camera Systems.

b. The ISTC will meet at least annually to discuss and receive updates on the current state of security systems, related policies, and emerging or new security and camera system technology. The ISTC may also convene as-needed upon request from the Associate Vice President of Public Safety.

c. The ISTC will be chaired by a representative from the Department of Public Safety.

d. The following departments will participate on the ISTC to provide subject matter expertise:

- Office of Information Technology (OIT)
- Architectural and Engineering Services
- Office of the General Counsel (OGC)
- Division of Student Affairs
- Office of Institutional Compliance and Ethics
- Human Resources, and
- Others by invitation as needed.

e. The Department of Public Safety's Integrated Security Technology Unit will:

- Schedule meetings with campus units who have requested a camera or cameras to discuss recommendations on camera types and associated costs. A representative from the requesting department, a member of the OIT network team (if necessary), and the University's security integrator will be included in the meeting.
- Develop the appropriate installation and signage, in consultation with the signage committee, for the Public Safety Camera System on University property.

- Oversee the initial instruction of Camera Control Managers and installers, as well as on-going guidance of those employees, as needed.
- Create procedures for storage, disposal, and retrieval of Content.
- Develop and execute the plan to ensure the integration of current and future systems according to established standards and the installation and signage protocols.
- Approve or deny requests to install new or replacement Public Safety Camera Systems.

4.2 Emergency Situations

During emergency situations, the Associate Vice President for Public Safety will:

a. Consult on and authorize Public Safety Camera System installations in the following situations:

- When it is required for an impending visit by a dignitary,
- When law enforcement or University officials are conducting an investigation, or
- When there is a significant, imminent risk to public security and/or University property or a campus emergency.

b. Immediately after an emergency installation has been authorized, the Chief of Staff and Vice President for University Affairs and the ISTC must be informed, as needed.

4.3 Content Ownership

All Content is owned by the University and is the responsibility of the Associate Vice President for Public Safety. The Associate Vice President for Public Safety will consult with the ISTC on decisions related to content that are deemed of high importance to the University community.

4.4 Placement and Limitations

a. Use of Public Safety Camera Systems will generally be limited to public areas.

b. Video recording must be not conducted in Personal Areas of the campus unless specifically authorized by the Associate Vice President for Public Safety, or by a search warrant or other lawful orders from a legitimate and duly authorized law enforcement entity.

c. Where Public Safety Camera Systems are permitted in Personal Areas, they will, to the maximum extent possible, be used narrowly to protect persons, money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.

d. Inoperative, placebo, or "dummy" security cameras shall not be installed or utilized, unless approved by the Chief of Staff and Vice President for University Affairs.

4.5 Monitoring and Review

a. The Department of Public Safety may monitor and review security camera feeds and recordings as needed to support investigations and to enhance public safety. It is not intended nor expected that Public Safety Camera Systems will be routinely monitored in real time.

b. With prior approval from the Associate Vice President for Public Safety, and in consultation with the Office of General Counsel, when appropriate, other University employees, including Camera Control Managers, may monitor and review security camera live feeds and recordings for purposes of public safety or internal investigations.

c. Monitoring individuals based on characteristics of race, sex, gender, gender identity, ethnicity, sexual orientation, age, disability, veteran's status, or other protected classification is prohibited. See University Policy 1060 (Non-Discrimination and Anti-Harassment) and University Policy 1065 (Sexual Harassment, Sexual Misconduct, Dating Violence, Domestic Violence, and Stalking) for more information.

4.6 Storing and Retaining Content

a. Video footage will be stored on servers accorded appropriate computer security with access by authorized OIT employees, contractors, or designated Camera Control Managers. The Associate Vice President for Public Safety, or designee, will authorize access to servers.

b. Content must be retained for thirty (30) days. After the 30-day retention period, the recordings may be erased, or recorded over, unless retained as part of a criminal investigation, court proceeding, or other authorized use as approved by the Office of General Counsel, the Associate Vice President for Public Safety, or as required by law. See University Policy 1030 (Litigation Hold) for more detail.

c. Requesting exceptions to the content retention period must be approved by the ISTC, or in an emergency situation, the Associate Vice President for Public Safety.

4.7 Use of Recordings

a. Public Safety Camera Systems must be used primarily for purposes of enhancing public safety.

b. Recordings may support disciplinary proceedings involving employees and/or students, or a civil suit or other proceeding involving person(s) whose activities are shown on the recording and relate to the proceeding.

4.8 Release of Recorded Material and Live Streaming

a. Requests for release of recorded material under Idaho's Open Records Law must be approved by the Associate Vice President of Communications and Marketing as detailed in the University Policy 1040 (Public Records).

b. Requests for release of recorded material set forth in subpoenas or other legal documents compelling disclosure must be reviewed and acted upon by the 1) Associate Vice President for Communications and Marketing, and 2) the Office of General Counsel.

4.9 Exceptions

Use of Public Safety Camera Systems beyond those described in this policy are prohibited. Individuals who have questions about the use of Public Safety Camera Systems not subject to this policy should direct those questions to the Associate Vice President of Public Safety.

Revision History

September 2015; July 2019