Preamble: This policy was created to regulate surveillance cameras and protect the legal and privacy interests of the University of Idaho and its community. [ed. 9-14]

General. The University of Idaho is committed to protecting the safety and property of the University community while respecting the privacy rights of our faculty, staff, students, and visitors. Cameras provide a visual deterrent to crime, assist with overall security measures, and increase the potential identification and apprehension of person(s) who commit criminal acts or violate University policies. The primary use-purpese of surveillance cameras is to record images for future identification of individuals and activity in the event of violations of law or policy. UI video surveillance security camera systems will not be actively monitored. [ed. 9-14]

A. Policy

This policy regulates the use of surveillance cameras to protect the legal and privacy interests of the University of Idaho and the University community. This policy applies to all University of Idaho persons and organizations using surveillance cameras systems and devices for recording activity, except as explicitly excluded below. [ed. 9-14]

The University of Idaho reserves the right to place video surveillance cameras on campus where necessary and appropriate. The University of Idaho respects the right to privacy of university community members and balances the right to privacy versus the safety needs of the campus community. The Office of Public Safety and Security ("University Security") is responsible for the creation and management of video surveillance camera records for law enforcement purposes, and is identified as the University’s law enforcement unit under the Family Educational Rights and Privacy Act ("FERPA"). All use of video surveillance cameras must be approved by University Security and is subject to oversight by that office. [ed. 9-14]

B. Procedures

B-1. Access and Use: Only those authorized by the Executive Director of Public Safety and Security or designee, will be involved in, or have access to surveillance camera data. [ed. 9-14]

   a. The use of dummy or placebo cameras is prohibited.
   b. University Security will have access to all surveillance camera data. [ed. 9-14]
   c. When an incident is suspected to have occurred, only authorized personnel may review the images from surveillance camera data. [ed. 9-14]
Only the Executive Director of Public Safety and Security or designee may authorize copies of security surveillance images. [ed. 9-14]

All requests to release surveillance records must be authorized by both the Office of General Counsel and the Executive Director of Public Safety and Security or designee. [ed. 9-14]

The University will not permit either the installation or use of cameras as a tool to monitor routine performance or management issues involving University personnel or the use of personal "webcam" or similar technology for surveillance purposes. Departments or units seeking to install or use cameras for this purpose must obtain approval from both University Security and Human Resources. If approved, employees of any department with surveillance cameras for this purpose will be notified of such installation. [ed. 9-14]

The use of personal "webcam" or similar technology for surveillance purposes is prohibited absent prior permission from the Executive Director of Public Safety & Security.

The recording of audio is prohibited.

Video recording will be conducted only in areas where the public does not have a reasonable expectation of privacy.

Video surveillance cameras shall not be specifically directed or zoomed into windows of any non-public areas of a residential building, including residence halls. Electronic shielding or other methods will be used to ensure compliance with this provision. [ed. 9-14]

In consultation with General Counsel and Information Technology Services ("ITS") staff, video surveillance implementation and policy exceptions will be reviewed by the Executive Director of Public Safety and Security on an annual basis. [ed. 9-14]

Unauthorized systems will be subject to removal at the expense of the department or unit in violation of these standards.

**B-2. Data and Access Log Storage:**

A log documenting access to and use of data stored in the University’s surveillance system will be maintained for a period of 12 months. [ed. 9-14]

Video tapes or other media will be stored and transported in a manner that preserves security. Current and archived tapes or media shall be kept locked and secured.

Recorded images shall be kept confidential and destroyed on a regular basis. Such images will be retained for a minimum of thirty (30) days and a maximum of one (1) year. Cameras purchased prior to the implementation of these standards will be granted an exception to the retention period above if recorded image retention is less than thirty (30) days. Recordings that, after review, merit retention for administrative or potential legal uses must be maintained for three (3) calendar years after the end of the year to which they relate. All recorded images used for an investigation or prosecution of a crime shall be further retained until the end of the proceeding and appeal period unless directed otherwise by a court of law.
B-3. **Device Procurement, Installation, and Maintenance:**

a. The installation of new surveillance cameras, their locations, and purpose must be approved in advance by the Executive Director of Public Safety and Security. A request for surveillance-camera installation must be submitted and approved prior to the purchase of equipment. Surveillance cameras must connect to the University's surveillance-camera system managed by University Security, in accordance with University product, installation, maintenance, and support policies. [ed. 9-14]

b. All costs associated with the purchase, installation, and maintenance of the system will be the responsibility of the requesting department or unit.

c. All authorized cameras and systems should be inspected annually by the department or unit to ensure they are in proper working condition and meet these guidelines. University Security may inspect all cameras and systems at any time to ensure compliance with this policy.

d. Signs stating that surveillance equipment is in use will be placed at main entries of buildings or near other appropriate areas.

C. **Excluded surveillance-camera systems and devices:** This policy does not apply to the use of video for non-surveillance-security purposes; examples include:

   [ed. 9-14]

   C-1. The academic use of cameras for educational purposes.

   C-2. Cameras used for research purposes, which are subject to policies regarding human subjects.

   C-3. Cameras used for journalistic purposes.

   C-4. Cameras used for capturing public events and performances.

   C-5. Construction web cameras.

   C-6. Cameras installed or used as part of criminal investigations, which are subject to appropriate Idaho and Federal laws.

   C-7. Webcams used for purposes of communication between specific persons.

D. **Contact Information.** For specific questions regarding this policy, contact The Office of Public Safety & Security: [www.uidaho.edu/public-safety-and-security; campus-security@uidaho.edu](mailto:campus-security@uidaho.edu)