SECTION: 4.0 Administrative

SUBJECT: Surveillance Camera

Background: This policy sets out the framework within which LC State will use surveillance cameras.

Point of Contact: Department of Campus Security, Information Technology

Other LCSC offices directly involved with implementation of this policy, or significantly affected by the policy: Vice President for Finance and Administration, Vice President for Student Affairs, Residence Life, Physical Plant, Student Union Building, and Human Resource Services

Date of approval by LCSC authority: February 1, 2021

Date of State Board Approval: N/A

Date of Most Recent Review: February 2021
Summary of Major Changes incorporated in this revision to the policy: Reformatted and added additional policy elements to clarify and conform with current practices.

Purpose: The primary purpose of this policy is to regulate and centralize the use of LC State camera surveillance systems used to observe and record public and personal areas.

1. **Policy:** LC State is committed to providing a safe and secure learning environment while safeguarding the privacy of College students, faculty, staff, community partners, and visitors. The use of surveillance cameras is part of an integrated security approach which includes a number of strategies including physical presence of security staff, access controls, and alarm systems. The primary use of LC State surveillance cameras is to record video images for use by law enforcement, the Department of Campus Security, and other College officials charged with investigating alleged violations of criminal law and College policy. Any interception, duplication, transmission, or other diversion of content for the purposes other than what is authorized by this policy is prohibited. The existence of this policy does not imply or guarantee surveillance 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.

2. **Definitions:**
   a. **Camera Control Managers:** Individuals designated by the College who are responsible for the College's recording, reviewing, and recovering of content.
   b. **Content:** All information, whether audio or video, captured by a College surveillance camera. This includes system logs, stills, snapshots, stop action, and video images whether transient, displayed, or recorded.
   c. **Personal Areas:** A location where a reasonable person would expect privacy, such as a residence hall living quarters, public restrooms, locker rooms, or other areas defined by law.

SECTION: 4.0 Administrative

SUBJECT: Surveillance Camera

3. **Roles and Responsibilities:**

a. **Integrated Security Technology Committee (ISTC)**
   i. 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 College security systems, including the surveillance camera system.
   ii. The ISTC will meet a 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 up request from the Director of Campus Security.
   iii. The ISTC will be chaired by a representative from the Department of Campus Security and may include representatives from Information Technology, Physical Plant, Residence Life, Risk Management, Human Resource Services, and other departments as appropriate.

b. Vice President for Student Affairs
   i. Approve or deny requests to install new or replacement College surveillance cameras.

c. **Department of Campus Security Responsibilities:**
   i. The Director of Campus Security will approve or deny requests to view camera surveillance content.
   ii. The Director of Campus Security will authorize access to servers in which video surveillance content is stored.
   iii. During emergency situations, the Director of Campus Security will:
      1. Consult on and authorize surveillance camera system installation when it is required for an impending visit by a dignitary; when law enforcement or College officials are conducting an investigation; when there is a significant, imminent risk to public security and/or College property, or in the event of a campus emergency.
      2. Immediately after an emergency installation has been authorized, the Vice President for Student Affairs and other applicable ISTC members must be informed, as needed.
   iv. **Content Ownership:** All content is owned by the College and is the responsibility of the Director of Campus Security. The Director of Campus Security will consult with the ISTC on decisions related to content that are deemed of high importance to the College community.
   v. **Testing and Maintenance:** Campus Security will verify that all cameras are functioning properly at least once per month. Inoperable equipment will be reported to Information Technology via a work-order request.

d. **Information Technology Responsibilities:**
   i. 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 and a member of the Department of Campus Security will be included in the meeting.

SECTION: 4.0 Administrative

SUBJECT: Surveillance Camera

ii. Develop the appropriate installation and signage, in consultation with the Department of Communications and Marketing, for the College surveillance camera system on College property.
iii. Oversee the initial instruction of camera control managers and installers, as well as ongoing guidance of those employees, as needed.
iv. Create procedures for storage, disposal, and retrieval of content.
v. Develop and execute the plan to ensure the integration of current and future systems according to established standards and the installation and signage protocols
vi. Maintain equipment to include all repairs as needed.

4. **Placement and Limitations**
   a. Use of Campus surveillance cameras will generally be limited to public areas.
   b. Video recording must not be conducted in personal areas of the campus unless specifically authorized by the Vice President for Student Affairs, or by a search warrant or other lawful order from a legitimate and duly authorized law enforcement entity.
   c. Where surveillance cameras 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" surveillance cameras shall not be installed or utilized, unless approved by the Vice President for Student Affairs.
   e. In compliance with relevant laws and regulations, signs will be displayed indicating that an area may be monitored. Signs indicating an area "is monitored by surveillance cameras" shall not be installed, or allowed to remain on campus.

5. **Monitoring and Review**
   a. The Department of Campus Security may monitor and review surveillance camera feeds and recordings as needed to support investigations and to enhance public safety. It is not intended nor expected that College surveillance cameras will be routinely monitored in real time.
   b. With prior approval from the Director of Campus Security, and in consultation with the Vice President for Student Affairs, when appropriate, other College employees may monitor and review surveillance camera live feeds and recordings for purpose of public safety or internal investigations.
   c. Monitoring individuals based on characteristics of race, sex, gender, gender identity, ethnicity, sexual orientation, age, disability, veterans status, or other protected classification is prohibited.
   d. This policy does not in any way imply or guarantee that video surveillance devices will be indefinitely operational or actively monitored at any time.

6. **Storing and Retaining Content**
   a. Content will be stored on servers accorded appropriate computer security with access by authorized IT employees, contractors, or other designated individuals approved by the Director of Campus Security.
   b. Content will be retained for at least thirty (30) days. After the 30-day retention period, the content may be maintained, erased, or recorded over. Content may be retained as part

of a criminal investigation, court proceeding, or other authorized uses approved by the Vice President for Student Affairs, or as required by law.

c. Requests to extend the content retention period must be approved by the Director of Campus Security.

7. **Use of Recordings**
   a. Surveillance camera content must not be used or disclosed for purposes other than those specified in this policy.
   b. All recordings and their contents are the copyrighted property of LC State and shall not be copied, distributed or used for any broadcast, performance or publication without the express written direction of the Vice President for Student Affairs, except when such actions are taken by law enforcement in conjunction with investigations or criminal prosecutions.
   c. 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.

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 and routed to the Vice President for Finance and Administration.
   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 Vice President of Finance and Administration and the Department of Communications and Marketing.

9. **Exceptions:** Use of Campus surveillance cameras 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 Director of Campus Security.