Office/Contact: Division of Technology and Security
Source: SDBOR Policy 7.1; University Policy 4:3
Link: https://public.powerdms.com/SDRegents/documents/1727287; https://www.sdstate.edu/sites/default/files/policies/upload/Equal-Opportunity-and-Non-Discrimination.pdf

SOUTH DAKOTA STATE UNIVERSITY
Policy and Procedure Manual

SUBJECT: Cameras used for Safety and Security
NUMBER: 10:6

1. Purpose

   This policy and its procedures regulate the use of camera equipment for the purposes of safety and security and the handling, viewing, retention, dissemination, and destruction of related records in accordance with SDBOR and University policy and state and federal law.

2. Policy

   a. This policy and its procedures apply to all employees and units of the University in the use of camera monitoring and recording and related systems. Legitimate uses of this technology are covered by University policies governing research with human subjects and are, therefore, excluded from this policy.

   b. The University is committed to enhancing the quality of life of the University community by integrating the best practices of safety and security with technology. A critical component of a comprehensive safety & security plan is the use of camera systems. Camera use and monitoring of public areas are intended to deter crime and assist in protecting the life, safety and property of the University community.

   c. Camera systems and records will be utilized in a professional, ethical, and legal manner. University personnel involved in the use of camera equipment and records must be appropriately trained and supervised in the responsible use of technology. All departments using these technologies are responsible for complying with this policy when implementing and operating cameras in their respective areas. Individuals who violate this policy will be subject to discipline or corrective action consistent with the rules governing the individual in question.

   d. The Division of Technology and Security, in consultation with the University Police Department ("UPD"), has the responsibility and authority as set forth herein to select, coordinate, install, operate, manage, and monitor all campus camera systems pursuant to this policy. Such use is subject to approval by the Vice President for Technology and Security, successor, or designee. With the exception of approved criminal investigation purposes, the decision to approve camera use will be based on the need to survey an area or event, not on an individual's presence or their personal status, including any protected status as defined in University Policy 4:3. More specifically:

i. The Vice President for Technology and Security, or designee, is responsible for establishing and disseminating written policies and procedures and assuring compliance with those policies and procedures.

ii. The Vice President for Technology and Security, or designee, in consultation with UPD, is responsible for determining the need for camera systems throughout the University and for providing technical standards and assistance in preparing proposals for the purchase and installation of camera systems.

iii. The Vice President for Technology and Security, or designee, is responsible for providing a project cost to the requesting department, including hardware, software and installation; for camera installation and server, storage and camera maintenance; and for implementing approved access permissions from UPD requests.

iv. The Vice President for Technology and Security, or designee, and the UPD are responsible for monitoring developments in the law and in security industry practices and technology to ensure that camera usage is consistent with best practice and complies with all federal and state laws.

v. The University is the owner of all video data, and the Vice President for Technology and Security, or designee, has the right to access and control all stored digital information and grant access to others as appropriate.

e. Camera systems for security and related systems will be limited to uses that do not violate the reasonable expectation of privacy, as defined by law and SDBOR and University policies, and may be used in situations and locations at the University where the security and safety of either property or persons would be enhanced. Cameras may be installed at the University for one or more of the following purposes:

i. Property Protection: to capture and store video on a remote device to record potential property theft or damage with the intent of capturing the perpetrator. (e.g. an unstaffed computer lab, an unstaffed science lab, or a parking lot.)

ii. Personal Safety: to capture and store video on a remote device to record crimes against persons with the intent of capturing the perpetrator. (e.g. a public walkway or a parking lot.)

iii. Remote monitoring: to stream live video in an area that requires remote monitoring in real time by a staff member who is in close proximity to that area. (e.g. a computer lab with multiple rooms that is being supported with one staff person.)

iv. To monitor activities in retail or other cash handling areas to reduce loss and assist investigations.

v. To monitor high risk areas or restricted access areas and locations.

vi. In response to an alarm, for special events, and in specific investigations authorized by law enforcement and approved by University or SDBOR General Counsel.

vii. Any other reason not listed above which is approved by the Vice President for Technology and Security, or designee.

f. Information obtained through camera systems will be used exclusively for official University purposes and may be used for law enforcement purposes. Information obtained through camera systems for non-law enforcement purposes will only be released when authorized by the Vice President for Technology and Security, or designee. A record log will be kept of all instances and access to use of recorded material. Information obtained in violation of this or other SDBOR or University policy may not be used in a disciplinary proceeding against a member of the University community. Nothing in this section is intended to limit the authority of authorized law enforcement activities.

g. All information obtained or observations made from the use of camera systems is considered confidential to the extent allowed by law. All appropriate measures must be taken to protect an individual's right to privacy and hold University information securely from creation through storage, transmission, use, and deletion.

h. The University Public Records Officer is responsible for reviewing all external requests to release records obtained through the camera system. The Public Records Officer will seek consultation and advice from University or SDBOR General Counsel related to these requests prior to the release of any records.

i. Under normal operating conditions, University camera systems are not monitored continuously. For the purposes of property protection and personal safety, access to live video or recorded video from cameras will be limited to persons authorized by the Vice President for Technology and Security, or designee. For the purpose of remote monitoring and approved local viewing, the live video stream may be monitored by the appropriate staff persons designated by the Vice President for Technology and Security, or designee. In all circumstances, any recorded video must comply with the recording storage and retention requirements applicable at the University.

j. Camera systems may have the capability to record video images and audible sounds. Typically, no audio will be recorded unless there is appropriate signage indicating that sounds may be recorded. However, audio may be recorded without such signage in areas where no one is permitted entry and when used as part of an investigation when approved in writing by the Vice President for Technology, or designee, with the advice of the Chief of Police, and approved by University or SDBOR General Counsel. Additionally, audio may be used in exigent circumstances without prior approval.

k. Unless being used for lawful criminal law enforcement surveillance, all video camera installations at the University shall be visible.

l. The installation and use of "dummy" cameras at the University is prohibited. Inoperable cameras must be repaired, replaced, or removed in a reasonable time.

m. All existing security camera systems shall be brought into compliance with this policy within twelve (12) months of its approval. After the twelve (12) month period, unapproved or nonconforming devices will be removed.

3. Procedures

   a. Requests for camera systems are forwarded to the Division of Technology and Security and must be approved by the Vice President for Technology and Security, or designee.

   b. If, upon determination of the Vice President for Technology and Security, or designee, the request identifies an institutional need for a camera, the IT resources will be provided to fund the proposed camera purpose and installation. If approved, the request will be added to the list of pending camera installation for scheduling.

   c. If the request is found not to meet an institutional need, the department requesting the camera system may purchase the camera. The camera(s), associated hardware, provider and installation location are required to meet the specifications set forth by the University and must be part of the University camera system.

   d. Upon approval, the approving authority will notify the Vice President for Technology and Security, or designee, of the approved request.

   e. The Vice President for Technology and Security, or designee, will manage placement of the camera(s) and required signage and will seek legal review by University or SDBOR General Counsel prior to final approval, placement, and use of the camera(s) and their related data as appropriate.

   f. The Vice President for Technology and Security, or designee, will review any complaints regarding the use of camera systems at the University and will determine compliance with this policy. Any determination by the Vice President for Technology and Security, or designee, may be appealed to the University President, who is the final arbiter.

   g. Data will be stored for the length of time constituent with South Dakota records storage requirements and law enforcement rules of evidence requirements.

4. Responsible Administrator

   The Vice President for Technology and Security, or designee, is responsible for the ad hoc and annual review of this policy. The University President is responsible for approval of this policy.

SOURCE: Approved by President on 04/15/2016. Revised; Approved by President on 02/16/2022. Revised 02/01/2024 (clerical).