

St. Cloud Technical & Community College

Policies and Procedures

Chapter S6 – Facilities Management

S6.7 Security Cameras

Update Revision Responsibility: Vice President for Administration

St. Cloud Technical and Community College (SCTCC) uses security cameras as one resource to enhance safety and security of persons and property. Additionally, security cameras may provide beneficial information for management and operations of SCTCC. All security camera installations must be approved in advance by designated SCTCC personnel, as described in this policy, except in the case of an emergency that makes such consultation impractical. Placement and use of security cameras must conform to applicable state and federal laws in addition to system and campus policies. Security cameras must not have audio monitoring or audio recording capabilities enabled. Video monitoring of public areas for security purposes must be limited to uses that do not violate the reasonable expectations of privacy, as defined by law.

Scope

This policy applies to all personnel and departments of SCTCC in the use of its equipment for video surveillance, monitoring, and recording on SCTCC-owned, leased or controlled properties; this policy does not apply to the use of video applications for academic, research, or educational purposes of SCTCC, or to security cameras installed by authorized financial institutions to monitor ATM machine usage on campus.

Management and Use of Security Cameras

The primary purpose of security cameras is to assist in the daily operations of campus security and safety in providing a safe and secure environment to the SCTCC community including students, employees, and visitors. Information obtained through video monitoring will be primarily used for security and law enforcement purposes. Information obtained through authorized surveillance may be used in support of disciplinary proceedings against SCTCC personnel or students, or by SCTCC for other appropriate purposes such as litigation.

The installation and monitoring of security cameras and equipment must be administered by the Director of Safety and Security (Director) as designated by the Vice President of Administration in a manner consistent with this policy. In consultation with the Vice President of Administration, the Director may authorize the use of video surveillance in a temporary location upon request of a college official if a specific safety or security risk exists; if the request concerns the investigation of individuals, the Director shall consult with the Vice President of Administration and the Office of General Counsel and/or human resources office of Labor Relations in the system office prior to approval. The Director shall consult with system legal counsel if requested by law enforcement to install video surveillance for a criminal investigation.

In public areas, signage giving notice of the use of security cameras shall be posted as deemed appropriate by the Director.

If concern over camera placement should arise, concerned persons may submit a petition to the Director for the removal or relocation of an existing camera. The Director will review petitions regarding camera location(s) and determine whether the policy is being followed. The Director will determine the appropriateness of an installation by weighing the concerns of the person(s) making the request and the safety and security of the entire community. The Director will weigh whether the potential increment in community security outweighs any likely infringement of individual privacy.

Principles

The following principles shall apply regarding the use of security cameras at SCTCC under this policy:

- All recording or monitoring of activities of individuals or groups by authorized SCTCC security cameras will be conducted in a manner consistent with applicable system and SCTCC policies, and will not be based on an individual's race, gender, ethnicity, sex, disability, or other personal characteristics that are protected by Board Policy 1.B.1.
- All recording or monitoring of video records will be conducted in a professional, ethical, and legal manner. Campus security and other personnel with authorized access to video recordings must receive a copy of this policy and will receive training on the effective, legal, and ethical use of the monitoring equipment upon assuming their role and at least annually thereafter.
- All recording or monitoring for security and safety purposes will be conducted only in areas where the public does not have a reasonable expectation of privacy. (e.g., not living spaces).
- Recorded images made by security cameras will be securely maintained by SCTCC pursuant to its records retention schedule. The alteration of video images is strictly prohibited.

Limiting Use, Disclosure, and Retention of Recordings

The Director is responsible for controlling access to the security cameras monitors and recordings consistent with applicable privacy laws. Security camera data maintained by SCTCC may be nonpublic or private data on individuals under the Minnesota Government Data Practices Act and the Family Educational Rights and Privacy Act (FERPA). (Video surveillance data may be nonpublic or private "security information" as defined by Minn. Stat. § 13.37 Subd. 1 (a) or private personnel or educational data pursuant to Minn. Stat. §§13.43, Subd. 4 and 13.32, Subd. 3, and FERPA, 20 USC 1232g, which may be accessed, used, and disclosed to third parties only as consistent with those laws.)

Nothing in this policy shall prevent reporting to law enforcement real-time observations of conduct that appears to constitute criminal activity.

Recorded images will be stored in a secure location with access by authorized personnel only. A log must be created and maintained by the Director of all instances of access to or use of surveillance records. The log must include the date and identification of the person or persons to whom access was granted.

