Minnesota State University, Mankato University Procedure	
Procedure Name: Camera and Video Footage Use	**Effective Date of Last Review:** January 2, 2018
Custodian of Procedure: Vice President for Student Affairs and Enrollment Management	**Date of Last Review:** September 2023
Date of Adoption: January 2, 2018	**Date of Next Review:** September 2030

PROCEDURE

To enhance security and the safety of the campus it may be appropriate to permanently install video devices on the campus. In such cases the following rules will apply:

1) Individual departments, programs, or organizations wishing to permanently install video cameras shall submit a written request to the appropriate dean, director, or department head with a statement justifying the benefit of installing such equipment. The statement must include the proposed number and location of the device(s), as well as the purpose of the installation, whether the location of the cameras involve recording of activity by students, employees or the general public, and the name and title of the individual who will be responsible for reviewing the locations. The source of funding for the installation must be specifically identified as part of the request.

2) The appropriate dean, director or department head will forward the request along with his/her recommendation to the Director of Security. If approved, the Director of Security or his/her designee will coordinate the installation with a designated contractor and IT Solutions.

3) A member of the campus community may file a written request to change the location or limit the visual range of a specific installation of video monitoring equipment based on a belief that it infringes on a reasonable expectation of privacy or other protected rights. The request shall be submitted to the Director of Security and shall (a) identify the location, (b) identify the right believed to be infringed, and (c) provide an explanation of how the video device installation infringes that right. The Director of Security or designee will review and respond to the request within twenty (20) business days after receipt. The response will be based on a reconsideration of the initial request to install the devices in light of the campus community member's concerns. The decision of the Director of Security can be appealed to the Vice President of Student Affairs and Enrollment Management.

4) The Director of Security will maintain a database listing the location of all the video surveillance system cameras.

5) Within six months of the effective date of this Policy, all existing uses of video monitoring and recording equipment on campus shall be brought into compliance with all aspects of this policy, including the approval process outlined in the preceding paragraph. Those which do not conform shall be removed.

6) The Director of Security may authorize any temporary installation as deemed necessary in connection with law enforcement investigation, to enhance security for special events or as otherwise deemed necessary to enhance security or aid law enforcement.

Operation

Monitors for video equipment shall be installed in controlled-access areas and shall not be viewable by unauthorized persons.

1) Security department personnel are authorized as the primary operators of the video camera security system. Other individuals who may have a legitimate need to review recorded material may be permitted to do so upon approval of the Director of Security or other staff as authorized by the Vice President of Student Affairs and Enrollment Management. This includes members of ITS and contractors hired to maintain the cameras.

2) Video surveillance and monitoring will be restricted to those areas for which camera installation is approved in accordance with this policy. In no case will surveillance or monitoring occur in areas where there is a reasonable expectation of privacy in accordance with accepted social norms, such as restrooms, locker rooms, or individual residential rooms.

3) If the Director of Security or designee determines it necessary to aid law enforcement in an investigation or search, recordings or image stills may be released to law enforcement, the media or the public. The release of video/images to the media or public will be coordinated with the Media Relations Director and be consistent with Minnesota Government Data Practices Act Minn. Stat. §13.

4) Requests for recordings made in connection with internal employee investigations or disciplinary matters shall be sent to the Director of Human Resources.

5) All requests from non-law enforcement sources external to the University for the release of information and results obtained through surveillance monitoring shall be submitted to the Director of Security.

6) For FERPA purposes, recordings with information about a specific student are considered law enforcement records unless the University uses the recording for discipline purposes or makes the recording part of the educational record.

7) All video surveillance operators shall:

- Provide written acknowledgement that they have read and understand this policy.
- Perform their duties in accordance with this policy.
- Access surveillance images only to the extent permitted by this policy.

8) Video surveillance operators are prohibited from:

- Monitoring individuals based on characteristics of race, gender, ethnicity, national origin, sexual orientation, disability, or other personal characteristics that are protected by Board Policy 1.B.1. All recording and monitoring of activities of individuals or groups by security cameras will be conducted in a manner consistent with applicable system and university policies.
- Viewing the interior of residential rooms through windows, doors, or other means.
- Duplicating images or permitting access to others to surveillance images except as specifically permitted by this policy.
- Using the equipment addressed in this policy for viewing, recording, accessing or otherwise using a video surveillance system or surveillance images in any manner that is inconsistent with this policy and/or outside the scope of the usage approved by the designated campus authority.

Storage

Surveillance images obtained pursuant to this policy must be stored in a secure location and configured to prevent their unauthorized access, modification, duplication, or destruction. Surveillance images obtained pursuant to this policy will normally be kept at least seven (7) days unless required for a student conduct case, university policy matter or for criminal investigation and prosecution purposes.

Exceptions

Exceptions to this policy may be made in the event of an emergency or other situation reasonably appearing to pose an imminent threat to the safety and security of the university community.

- University-sanctioned video recording of University athletic or performing arts events is excluded from this policy.

- There are exceptions where cameras may be installed in testing locations, lab environments, simulation centers or other academic environments. All exceptions must be approved by the Director of Security or designee.
- Web cameras used in an office or laboratory space are excluded from this policy as long as anyone who would be on the camera are aware of the device.
- Video conference equipment installed on campus is exempt from the policy.
- Web cameras installed by the University to communicate construction progress or other University-related project of general shall be coordinated through the Security Department.
- The use of drones shall be governed by applicable policies/procedures of Minnesota State Colleges and Universities, this University, and FAA rules and regulations.
- Nothing in this policy applies to businesses that are located on campus property that are not controlled by the University.

Violations

Any individual who has concerns about the possible violation of this policy may discuss the matter with the Director of Security. Any individual found to have violated this policy may be referred for discipline under the applicable personnel or student conduct process.

Individuals who are believed to have tampered with or destroyed security camera equipment or recordings, or individuals who have accessed security camera records without authorization, may be subject to discipline under the applicable personnel or student conduct process and criminal prosecution, as appropriate.