University of Minnesota
Video Surveillance (CCTV) and Card Access (CA) Monitoring, Recording, and Data Retrieval Policy

Purpose:

The purpose of these policies and procedures is to provide guidance regarding the use of CCTV/Card Access on the University of Minnesota campuses. CCTV/Card Access is used to enhance security, safety and the quality of life of the campus communities by integrating the best practices of "virtual patrolling" with state-of-the-art technology.

This policy applies to all University of Minnesota affiliated campuses and centers state-wide in the use of CCTV/Card Access monitoring and recording. Legitimate research is excluded from this policy if covered by University policies governing ethical research policies and procedures.

Policy Statement:

The University of Minnesota is using CCTV/Card Access to monitor public areas in order to deter crime and to assist the University departments in providing for the security and safety of individuals and property of the University community. Any diversion of security technologies for other purposes would undermine the acceptability of these resources for critical safety goals and is therefore prohibited.

Monitoring of public areas for security purposes will be conducted in a manner consistent with all existing University policies, including the Non-Discrimination Policy, the Sexual Harassment Policy, and other relevant policies. The Standard Operating Procedures for video monitoring prohibits monitoring based on the characteristics and classifications contained in the Non-Discrimination Policy (e.g., race, gender, sexual orientation, national origin, disability, etc.)

Monitoring of public areas for security purposes at the University is limited to uses that do not violate the reasonable expectation of privacy as defined by law.

To ensure privacy, wherever practicable the cameras are prevented from focusing or dwelling on domestic accommodations. Where it is not practicable to prevent cameras from focusing on such areas appropriate training will be given to the center monitors to ensure that they are made aware that they should not be monitoring such areas.
Staff involved in CCTV/Card Access monitoring will be appropriately trained and supervised by Public Safety in the responsible use of this technology. CCTV/Card Access monitoring for security purposes will be conducted in a professional, ethical, and legal manner. Violations of the Standard Operating Procedure for CCTV/Card Access monitoring referenced in this policy will result in disciplinary action consistent with the rules and regulations governing employees of the University.

Information obtained through CCTV/Card Access monitoring will be used exclusively for safety, security, and law enforcement purposes. Recorded data will be stored in a secure location with access by authorized staff only. Entities capable of requesting this data include the University of Minnesota Police Department, Office of the General Counsel, Human Resources Office and the Department of Audits. Requests are to be made in writing for the purpose of conducting formal investigations.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against a member of the University faculty, staff or student body.

**Responsibilities:**

Public Safety oversees and coordinates the use of CCTV/Card Access monitoring. Public Safety authorizes all CCTV/Card Access monitoring for safety and security purposes on the campus.

Employees or subcontractors under the direction of Public Safety are responsible for the daily operation of the cameras and readers. They will follow all University policies, procedures, and guidelines in the monitoring of cameras and readers. No unauthorized staff will operate the system at any time.

Legitimate safety and security purposes for CCTV/Card Access monitoring include, but are not limited to:

- Protection of individuals, property and buildings;
- Confirmation of alarms;
- Patrol of public areas;
- Investigation of criminal activity.

Illegitimate safety and security purposes for CCTV/Card Access monitoring include, but are not limited to:

- Monitoring political and religious activities;
- Employee and/or student evaluations.
- Informal or unauthorized investigations.
**Procedures:**

**Department of Central Security staff will:**

- Conduct video observation of public areas that are in plain view of others.
- Be trained in the technical, legal, and ethical parameters of appropriate CCTV/Card Access use.
- Monitor based on suspicious behavior, NOT group characteristics.
- The University of Minnesota police dispatch will be notified immediately whenever any suspicious, criminal or life-threatening activity is observed.
- Monitors must document all suspicious, criminal or life-threatening activities in detailed incident logs.

**Department of Central Security staff will not:**

- Monitor based on race, gender, sexual orientation, national origin, disability, etc.
- Monitor unauthorized areas through the CCTV/Card Access equipment (e.g. Living spaces).
- Release CCTV/Card Access data without written approval for a formal investigation.

**Quality Assurance Procedures:**

- Security management and monitoring center supervisory staff will provide ongoing oversight of CCTV/Card Access operator activities and performance. Security department management will also conduct periodic, unscheduled reviews of the network digital recorder.

- Supervisors must supply each center monitor with a copy of the University CCTV/Card Access Policies and Standard Operating Procedures.

- Periodically and without prior notice, management will require staff to demonstrate their knowledge and understanding of relevant policies, procedures, and technical skills.

- The Department of Public Safety will monitor new developments in the relevant law and in security industry practices to ensure that CCTV/Card Access monitoring at the University is consistent with the highest standards and protections.
• Department of Public Safety management will assure that responsible and proper CCTV/Card Access monitoring practices by staff is continuous.
• The Department of Public Safety will limit camera positions and views of residential housing. Any view given to the housing will be no greater than what is available with unaided vision. Furthermore the view of a residential housing facility must not violate the standard of "reasonable expectation of privacy."
• The Department of Public Safety, Department of Central Security, and/or additional future central security monitoring locations will be configured to prevent camera operators tampering with or duplicating recorded information.
• Recorded data will be stored for a period of at least 30 days and will then be erased, unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Assistant Vice President of Public Safety.
• Digital images and access data will be stored in a secure location with access by authorized personnel only.
• Staff will conduct video observation of areas only in plain view.
• Mobile video equipment may be used in criminal investigations. Mobile video equipment will only be used in specific instances creating significant risk to public safety, security, and property as authorized in writing by the Assistant Vice President for Public Safety.
• Portable hidden cameras with recording equipment will only be used for criminal investigation by the University Police Detective Unit with the approval of the Assistant Vice President of Public Safety.

**Documentation:**

Each Incident that is supported or initiated by CCTV/Card Access will be documented. In the record of the incident, the operator will enter:

• That CCTV/Card Access was used on the incident;
• The specific camera and/or reader used; and
• Any pertinent information gathered by CCTV/Card Access.

© 2005 The University of Minnesota. All rights reserved.