SPG U-M Standard Practice Guide

UNIVERSITY OF MICHIGAN

Proper Use of Security Cameras

606.01

I. Overview

The University of Michigan seeks to provide its community with a safe and secure environment. When successfully deployed, security camera systems enhance overall campus safety and security, deter crime, and otherwise support the protection of people and property. A *security camera* is defined as video surveillance technology that records people's activities in order to detect, deter, prevent, or investigate crime or other threats to public safety.

The university has a significant responsibility to take appropriate steps to protect personal privacy and civil liberties when it operates security camera systems. Accordingly, no security camera may be installed on the University of Michigan campus in any location for which there is a reasonable expectation of privacy. Also, such installations must not impinge on or unduly constrain the academic freedom or civil liberties of community members or their freedom of assembly and expression.

II. Purpose of Policy

The purpose of this policy is to regulate the installation and appropriate uses of security cameras by any U-M unit, including the retention and release of recorded images. This policy applies to cameras installed or activated—permanently or on a temporary basis—specifically for purposes of enhancing campus safety and security, irrespective of the specific camera technology or whether they are monitored in real time.

III. Scope and Exclusions

Efforts to promote campus safety and security by the installation of security cameras are primarily focused on, but not limited to, protection of individuals—including students, faculty, staff, and visitors--and monitoring of:

- University-owned and/or operated property and buildings;
- Rooms and labs containing high value equipment or information;
- Cash-handling areas where money is exchanged, such as ATMs and cashier locations; and
- Common areas and areas accessible to the public.

This policy applies to all U-M units, departments, and employees, including contractors, with respect to the installation, operation, and monitoring of security cameras.

Security camera systems generally cannot be installed in areas where there is a reasonable expectation of privacy. These areas include, but are not limited to:

- Restrooms
- Locker rooms
- Occupied student residential rooms.

Video cameras are used for a variety of purposes at U-M. Consequently, this policy does not apply to the following applications where cameras are deployed for a primary purpose other than security:

- Clinical patient care
- Human subjects research
- Teaching and learning
- Video conferencing

- Human resources
- U-M Police Department (UMPD) in-car and covert cameras utilized for specific law enforcement purposes where relevant federal and state laws, statutes, and ordinances govern the use of electronic recording by law enforcement agencies.

Security camera systems should not enable audio recording.

The executive vice president and chief financial officer (EVP/CFO), in consultation with the executive director of the Division of Public Safety and Security (DPSS) and the vice president and general counsel, may grant exceptions to this policy. Exceptions, including their rationale, should be documented in writing and included in the inventory specified in Section V.

In cases where exceptions to this policy are necessary due to contractual requirements, approval must be obtained from the Office of the General Counsel and the unit's dean, director, or delegated executive authority.

Digital records created by security cameras are exempt from the provisions of SPG 601.8-1, Identification, Maintenance, and Preservation of Digital Records.

IV. Policy

Video surveillance records are defined as institutional data in accordance with SPG 601.12, Institutional Data Resource Management Policy. Specifically, images recorded by security camera systems are considered sensitive information whose confidentiality, integrity, and availability should be protected under SPG 601.27, Information Security Policy. Security camera recordings will be considered university data that fall under the aegis of the Business/Finance data steward (U-M Data Administration Guidelines for Institutional Data Resources). Security camera systems will be required to implement security safeguards appropriate to the sensitivity, criticality, and level of identified risk of stored video images and recordings.

Covert cameras are hidden or concealed with no signage and usually are installed for a specific and targeted intent. For purposes of safety and security investigations, only UMPD may install covert cameras for criminal investigations. Such surveillance must be authorized in writing by the DPSS executive director or delegated authority for each discrete incident and reported to the EVP/CFO prior to the start of the surveillance.

All units that install or maintain security camera systems are required to register their systems with the Office of the EVP/CFO. Completed unit registrations, including a specified business need, camera locations, and image retention period if different from this policy, must be approved by the appropriate dean, director, or delegated executive authority and submitted to the EVP/CFO. Registrations should note and explain any significant policy or process variations from this policy. No sub-unit should operate any security cameras in a manner that is more permissive than its unit's published policy without express approval from the respective dean or director. Deans and directors are required to annually review and recertify their unit's policy, procedures, and compliance.

University Human Resources (UHR) in conjunction with the Office of the General Counsel is responsible for any video surveillance related to human resources uses.

V. Oversight and Governance

The executive vice president and chief financial officer or a delegated executive authority shall convene on at least an annual basis a multi-unit campus oversight committee with faculty, administrative, and student representation that has the responsibility to:

1. At least once every three years, review and revise this policy and related standards, guidelines, and procedures;
2. Review and approve major amendments to this policy; and
3. Provide periodic updates to the U-M community about campus security camera systems for enhanced transparency.

The EVP/CFO, or delegated executive authority, will:

1. Serve as the central repository for unit templates with unit-specific policies and procedures;
2. Maintain an up-to-date comprehensive inventory of permanent camera installations and image storage locations to facilitate UMPD access to recorded images of possible crimes or incidents that require investigation;
3. Provide periodic administrative updates and guidance to security camera systems operators.

VI. Operator Roles and Responsibilities

Access to camera systems must be strictly controlled. The authorized users or operators of security camera systems are staff members who have been assigned responsibility by deans, directors, or other delegated executive authorities. Once authorized, operators are responsible for the installation, management, operation, maintenance, and use of security cameras and surveillance systems. Each unit that maintains a camera system is required to maintain an up-to-date list of the unit's authorized personnel with access to the system and any live or recorded images. Authorized personnel should generally consist only of the designated executive authority and security camera system operators and supervisors.

Security camera system operators must be trained and supervised in the responsible and effective use of these systems and technology, including the technical, legal, and ethical parameters of such use. Operators will receive campus security training from UMPD to help ensure U-M compliance with relevant provisions of the federal Clery Campus Security Act. UMPD will maintain records of training for three years.

Operators must receive a copy of this policy and related standards of appropriate use, and must sign that they have read and agree to the operator code of conduct.

Upon staff separation for whatever reason, units must ensure that camera operator access privileges are withdrawn within 24 hours of termination of employment.

VII. Authorization and Approval of New Installations

All new installations of security cameras scheduled after the effective date of this policy must be in compliance with the terms and conditions of this policy and related standards and must meet the minimum technical specifications identified in the U-M Security Cameras Technical Standard. Units must have their completed unit registration, endorsed by their respective dean, director, or delegated executive authority, approved by the DPSS executive director and filed with the Office of the EVP/CFOprior to moving forward with the installation.

Existing installations must be brought into compliance with this policy and related standards at the time units initiate replacement or significant upgrades of camera systems.

In facilities where common spaces are being considered, consultation with all units in the facility must occur before a new installation can be authorized.

VIII. Recorded Images Retention, Access, and Release

Security camera system operators are responsible to appropriately protect the privacy of personal information that may have been captured by cameras under their control. The Retention and Release of Security Camera Recorded Images Standard defines specific terms and conditions for allowing other parties to access these images or to release the images, including guidelines for the sharing of images internal to U-M departments.

All recorded images generated by U-M security cameras must be stored in a secure location established by the operating unit, accessible only to authorized and trained staff members, and configured to prevent unauthorized modification, duplication, or destruction.

Recorded images should be retained for no more than 30 days unless there is a demonstrated business need, grantor requirement, or the images are part of an ongoing criminal or civil court proceeding, employment investigation, legal hold, or court order. Recordings must be erased or recorded over after 30 days in the absence of a compelling reason to retain or a request from the DPSS executive director, Office of the General Counsel or the EVP/CFO.

Other requests for access to or release of recorded images must be forwarded to the EVP/CFO or designee, who will review the request and make the final determination. No unit personnel, including the dean, director, or designated executive authority, can make such determination.

Security camera systems operators must maintain a log of all instances of access to and release of recorded material.

IX. Violations and Sanctions

Violations of this policy by operators of security camera systems will be considered misconduct on the part of the employee who will be subject to institutional sanctions up to and including termination of appointment.

X. Monitoring Compliance

This policy governs all new unit and departmental security camera systems with planned installation as of the policy's effective date.

All units that maintain security camera systems should designate an administrator to ensure that records that validate compliance with this policy are retained for a period up to two years.

Compliance with this SPG may be subject to review by University Audits or other institutional compliance areas.

XI. Related Standards

- Operator Code of Conduct
- Technical Standard
- Retention and release of video security camera recorded images

SPG number:
606.01

Date issued:
June 10, 2013

Next review date:
June 11, 2018

Applies to:
All Faculty, Staff, and Students

Approved by:
Provost and Executive Vice President for Academic Affairs, Executive Vice President and Chief Financial Officer, Executive Vice President for Medical Affairs, and Vice President for Research

Owner:
Provost and Executive Vice President for Academic Affairs, Executive Vice President and Chief Financial Officer, Executive Vice President for Medical Affairs, and Vice President for Research

Related policies:
Freedom of Speech and Artistic Expression
Identification, Maintenance, and Preservation of Digital Records Created by University of Michigan
Information Security Policy
Institutional Data Resource Management Policy
Privacy and the Need to Monitor and Access Records
Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan