

Miami University

Fixed/Installed Camera policy 5/18/07

MUPIM addition (16.4 Buildings and Grounds or new section 16.19 Fixed/Installed Cameras):

The University may install observation cameras on University property to protect resources, enhance safety and assist in the educational mission as provided in this policy. The University will not install observation cameras on University property in faculty/staff offices or in non-public areas of residence halls. If an observation camera is installed where identification of personal images is possible, the camera must be accompanied by appropriate signage indicating the presence of the camera and whether or not it is monitored in real time.

Purchase and installation of camera equipment to protect resources or enhance safety requires the initial approval of the appropriate vice president. Purchase and installation of camera equipment for use in research must be approved by the Office of Advancement for Research and Scholarship. Purchase and installation of camera equipment for use in classrooms or to otherwise assist in the educational mission must be approved by the Provost. All requests must first be approved by the Space Utilization Group (all indoor installations) or the Campus Planning Committee (all outdoor installations). The Department of Physical Facilities and the University Information Security Office are responsible for determining equipment, signage and placement standards.

[MUPIM proposed addition ends here; subsequent verbiage is under revision for separate policies/procedures document]

RATIONALE:

Increased attention to protection of human and physical resources around the university as well as requests for information e.g., traffic and weather conditions has resulted in the need for quickly deployed, permanently installed and easily maintained security and convenience camera systems. Digital recording devices and digital monitoring devices provide a very cost effective solution and are readily available. However, these devices are being installed without regard for privacy or other requirements. Also, placing these devices on the data network without proper information security consideration or configuration could result in access to the system or to information being collected on the system by unauthorized users. This is particularly critical for cameras that are protecting valuable resources (e.g., research-related, monetary, equipment assets) and may collect information to deter or record misconduct. In order to ensure systems are being accessed only by the

minimum persons required, equipment and software must be reviewed by the ISO to determine if the requested system can be secured, methods that can be used to access the system from on and off campus, and potential impact on network traffic when the system is placed in service.

All requests approved by the appropriate Vice President and Space Utilization Group (all indoor installations) or the Campus Planning Committee (all outdoor installations), whether or not the devices will be connected to MUnet, must be reviewed by Physical Facilities and the University's Information Security Officer in order to insure that standards regarding equipment and placement are followed. All academic research and teaching requests for use of cameras require prior approval by the governing entity for research or teaching.

All existing uses of cameras should be brought into compliance with this policy within 12 months of the approval of this policy. Unapproved or non-conforming devices may be removed.

This policy does not address the installation or use of web cameras for communication purposes or the installation or use of cameras for law enforcement purposes.

IT STANDARDS AND DEFINITIONS:

Policy Cameras. Devices attached to the network for purposes of protecting valuable resources and which transmit identifiable personal images to deter or record misconduct. These devices should not be placed in such a location as to otherwise invade personal privacy. Access to images is restricted. Those authorized to have access to the images will receive a copy of these guidelines and must provide acknowledgement that they have read and understand them.

Public Convenience Cameras. Devices attached to the network for purposes of public convenience (to view, for example, construction project progress, weather conditions, or traffic conditions) should not invade personal privacy and therefore, should be placed far enough away that identifiable personal images are not transmitted. Such devices will not have storage capabilities since there is not a reasonable expectation that they will capture identifiable personal images for use in policy violations. Access to images is not restricted; they are viewable by the general public.

Standard Approved Devices. The devices approved for installation are specified in Appendix A, "Equipment Standards and Specifications." The list will be updated periodically. The Information Security Officer and Senior Director for Computing and Communication Services (or their designees) are responsible for maintaining the list of approved equipment.

Location and Signage. Devices will be in plain view and signage must be installed that indicates whether or not 24/7 monitoring of activities is provided (Example - SECURITY CAMERAS IN USE. These cameras are not actively monitored.”)

Cameras will not be installed in private areas of residence halls. Signage shall be governed by Physical Facilities in accordance with university procedures. The following chart outlines general standards regarding locations.

Device Location	Permitted; require approval	Not Permitted	Notes
Hand-held mobile cameras used for research, teaching, class work or personal use			Not covered by this document
Web cameras for communication purposes in faculty and staff private offices			Not covered by this document
Construction cameras	X		Monitor construction progress; no personally identifiable images; no recording capability
Public convenience cameras	X		Monitor weather or traffic; no personally identifiable images; no recording capability
Classrooms, teaching laboratories, or other areas in academic buildings or field sites	X		If approval for academic or research purposes is granted by OARS (IRB, IACUC, Research Compliance as appropriate), or for teaching purposes by the Provost, then installation is governed by this document; recording capability.
Research lab or location on University property	X		Must be approved first by OARS (IRB, IACUC, Research Compliance as appropriate). Installation is governed by this document; recording capability.
Computer labs	X		For protection of equipment; recording capability
Faculty/staff private offices		X	Permanent installation of policy cameras in such locations is prohibited; Web cameras for communication purposes are not covered by this document.
Business locations; Libraries	X		For protection of valuable assets; may have unique retention periods; recording capability
Residence Halls, interior	X		For protection of valuable assets only in public areas of residence halls (i.e. – computer labs or lecture halls)
Residence Halls, exterior	X		Monitor entrance/exit; recording capability
Dining Halls, interior & exterior	X		Recording capability
Parking garage	X		24/7 real-time monitoring required if purpose is to enhance security

Academic Research and Teaching. Approval for camera installation does not constitute approval for use in academic research and teaching. Approval for use of cameras in research is governed by OARS (including the Institutional Review Board for Human Subjects (IRB), IACUC, and Research Compliance, as appropriate). The Provost or designee approves requests for use of cameras in teaching. Approval must first be obtained by the appropriate entity mentioned above. If the request to use fixed/installed cameras in research or teaching situations is approved, installation is governed by this document.

Installation. Installation of policy or public convenience cameras must be approved by the ISO (or the Video Camera Review Committee coordinated by the ISO for camera protocol), prior to installation. Physical Facilities and IT Services will consult on the placement of the equipment and, if applicable, connection to MUnet. Physical Facilities will be the final authority with respect to issues of placement and appearance of the device in accordance with University building standards.

Access to Images. Access to data recorded by the installed devices is governed by the *Data Stewardship Policy* and *Responsible Use of Computing Resources at Miami University*. Use of and access to research data is governed by the University under the Ohio Public Records Act and similar statutes, and adherence to those laws is under the jurisdiction of OARS and the University Counsel's office.

Retention. In accordance with the University's records retention policy, digital images are to be retained for a minimum of seven days up to a maximum of thirty days for non-research related purposes. Exceptions will be allowable under justified circumstances as determined by the University Secretary. Retention of digital images captured for research purposes is governed by OARS in consultation with the University Secretary.

FERPA. Any recording that includes personally-identifiable images of students is governed by the Family Education Right to Privacy Act (FERPA). The student's right to privacy must be protected.

PROCEDURES:

Request purchase and installation of policy or convenience cameras. Submit a completed Miami University Project & Space Utilization Request Form to the Space Utilization Group (SUG) for approval.

Review and approval. After gaining SUG approval, the request is sent to the Information Security Officer (ISO). The ISO is responsible for reviewing camera requests in consultation with the Director of Small Construction Projects, Physical Facilities.

This must be done in advance of purchasing any equipment or scheduling any installation work. Requester will be contacted by the ISO to determine that auditing capabilities, system password protection, and user access control measures are provided and effective. Only standard, supported equipment can be installed. Requesting departments are responsible for funding the equipment purchase, installation, maintenance, and lifecycle replacement costs. The need to consult with others prior to a decision is made on a case by case basis.

Equipment Purchase. Once a request is approved by the Information Security Officer or designee, the requester is notified that the request is approved, the equipment will be purchased, and installation will be scheduled. The requester provides the departmental account number to be charged.

Replacements and Upgrades. Any system replacements or upgrades must also be reviewed and approved by the Information Security Officer or designee and, as needed, the Director of Small Construction Projects, Physical Facilities. The requesting department is responsible for funding and coordinating all service and replacement needs. Contact the IT Services Support Desk (513-529-7900 or supportdesk@muohio.edu) to request replacement or upgrade. Provide the following information:

- Location(s) of existing security cameras
- Justification for the request

Repairs and Maintenance. The original requesting department is responsible for funding and coordinating repair and maintenance needs. Contact the IT Services Support Desk with a request for repair or maintenance (513-529-7900 or supportdesk@muohio.edu). Provide the following information:

- Location(s) of existing equipment
- Explanation of the issue
- Account number to be charged

Appeals Process. Requests for installation that are denied by the ISO may be appealed to the Vice President for Information Technology. Contact the secretary at 529-8338 or contact the Deputy CIO at 529-5327.

Planning and Management. A small planning Video Camera Review Committee will provide oversight and management in order to (1) identify the necessary equipment and installation standards and (2) ensure consistency in the application of the guidelines. The committee shall be comprised of the following representatives:

- Physical Facilities

- IT Services Networking
- Regional Campuses

An inventory of all cameras installed at Miami University will be maintained by the ISO and periodically reviewed for improvements in consistency of placement. In the event that only a few locations of a particular type, e.g., computer labs, have a camera installed, the installations should be reviewed to determine whether all locations should receive cameras, or none, or continue as is.

Proliferation of cameras may result in tightening of standards for installation or changes to guidelines in the event that this is deemed advisable by the university administration.

APPROVAL(S) AND DATE(S):

Approved by IT Services: March 19, 2007

Approved by Physical Facilities: February 21, 2007

Approved by the University Senate: March 19, 2007

Version number: 1.0

Effective Date for Policy: May 18, 2007

REVISIONS (Dates): [Summarize revisions, rationale; specify approvals given and dates once document receives initial approvals.]

APPENDIX A: EQUIPMENT STANDARDS AND SPECIFICATIONS

[Specify manufacturer, model, digital recording media, and other identifying characteristics. Indicate date approved and date for review. Note that any requirements for image storage must be met via digital recording equipment, not video tape recording. Standards should specify whether any central digital storage capability will be provided.]

Denial of Access. IP addressable cameras and IP addressable digital recorders making a connection to MUnet must allow for denial of access by other than those users specifically included in a system Access Control List.

Access through VPN. All access to IP addressable cameras and associated digital recorders used to deter or record misconduct will be accomplished through the centrally managed Virtual Private Network (VPN).

Audit Reporting of Accesses. Digital recorders used to collect and store identifiable personal images should be configurable to allow audit reporting of access to the recorder.

Storage Standards. Digital recorders used to collect and store identifiable personal images should:

- include technology for "watermarking" of files in order to be suitable for evidentiary documentation
- include capability for transfer of stored images to external storage media
- not require vendor specific/proprietary applications or software clients for viewing live or stored images
- provide a minimum of 7 days of image storage from all connected cameras in the recording device; exceptions will be made on an individual basis by the ISO
- provide for tracking of recordings to prove chain of evidence
- provide protection of equipment to preclude removal of evidence by other than the responsible person.

Equipment and Cabling Specifications for Standard Approved Devices.

Cabling Installation Standards. Camera devices and their associated wiring shall be performed in accordance with MU IT Services Cabling Installation guidelines and procedures. Current standards are detailed in IT Services 16710, and 16740 documents. Contact Network Services at 529-9672 or Telecommunications at 529-1277 for the current revision of these documents.