Video and Electronic Surveillance
PS-02

About This Policy

Effective Date:
01-01-2012

Last Updated:
04-29-2014

Responsible University Office:
Public Safety & Institutional Assurance

Responsible University Administrator:
Office of the Executive Vice President for University Academic Affairs

Policy Contact:
security@iu.edu

Back to top

Scope

This policy applies to all video and electronic surveillance systems that monitor or record Indiana University facilities and/or community members using those facilities, regardless of system ownership or the owner's affiliation with the university.
Video and electronic surveillance systems outside the scope of this policy:

- Systems used in health treatment settings (governed instead by the Health Insurance Portability and Accountability Act (HIPAA)).
- Systems used for human subjects-based research (as "research" is defined in federal law and in university policy governing research; controlled instead by campus Institutional Review Boards (IRB)).
- Systems deployed specifically for law enforcement purposes. The campus Chief of Police shall continue to oversee the operation and use of those systems. However, campus police's access or use of any video and electronic surveillance systems and associated surveillance information within this policy's scope shall be covered by this policy.
- Systems used to observe, capture, or analyze Information Technology telecommunications traffic (governed instead by university policy IT-07, Privacy of Electronic Information and Information Technology Resources).

In addition, this policy does not address video and/or electronic surveillance devices when used for the following purposes:

- deliver education;
- conduct teaching, non-human subjects-based research, or creative activity;
- conduct video conferencing;
- record public performances, events, or interviews;
- record practices or rehearsals;
- record news or press coverage; or
- produce promotional materials.

However, in the event any such devices are to be used for any other purpose not specifically outside the scope of this policy, then this policy shall then govern.

For further assistance in the types of video and electronic surveillance systems covered by the policy, see Related Information below.

Back to top

Policy Statement

Indiana University respects the privacy of individuals who are using university buildings or on university grounds. The university will take pragmatic and measured steps to provide an efficient, effective, safe, and secure environment while avoiding unnecessary intrusions upon academic freedom or individual civil liberties including privacy, freedom of expression, and freedom of assembly.
The approval, installation, operation and use of all video and electronic surveillance systems shall comply with all applicable state and federal laws, and all institutional policies and standards, including but not limited to those laws and policies that prohibit discrimination and harassment and that honor an individual's reasonable expectation of privacy in accordance with accepted social norms.
Back to top
Approval, Installation, and Operation

- Video and electronic surveillance systems shall only be installed and operated following prior review and written approval by the designated campus authority and only as outlined in this policy.
- Exceptions to the prior review and written approval requirement may be made in the event of an emergency or an imminent threat to the safety and security of the university community, and only as outlined in this policy.
- Video and electronic surveillance systems shall be listed and tracked in a master inventory maintained for each campus.
- Video surveillance systems shall be installed, administered, and managed centrally, either university-wide or per-campus.
- Video and electronic surveillance systems shall be installed and operated by a limited number of authorized operators who:
    1. demonstrate a legitimate need for such access consistent with the purposes of this policy; and
    2. are appropriately trained and supervised in the responsible use of these systems.
- Video and electronic surveillance systems that exist at the time of this policy's approval shall be brought into compliance with this policy within 12 months.

Back to top
Appropriate and Prohibited Uses

- Video and electronic surveillance systems shall not be installed in or used to monitor or record areas where there is a reasonable expectation of privacy in accordance with accepted social norms. These areas include but are not limited to restrooms, locker rooms, individual residential rooms, changing or dressing rooms, and health treatment rooms.
- Video and electronic surveillance systems shall not be installed in or used to monitor or record residential hallways, residential lounges, or the insides of campus daycare facilities unless specific safety or security risks have been demonstrated, and then only with prior explicit review and approval as outlined in this policy.
- Video and electronic surveillance systems shall not be used to record audio unless prior approval is obtained from the Chief Privacy Officer and the Office of the General Counsel, in addition to normal designated campus authority approval.
- Video surveillance systems shall not be used to monitor or record sensitive institutional or personal information which may be found, for example, on an individual's workspaces, on computer or other electronic displays.
- Surveillance information obtained through video and electronic surveillance systems shall not be accessed, used, or disclosed except as outlined in this policy.

Back to top

Reason For Policy

The University may install video and electronic surveillance systems for a number of purposes including public safety, security, public convenience, and operational effectiveness. These systems must be deployed and managed in accordance with applicable laws and the philosophies and values of Indiana University.

Back to top

Procedure

This section contains a summary of this policy's procedures. For detailed procedures, please see PS-02.1 Procedures – Video and Electronic Surveillance.

1. **Approval and installation**
   Video and electronic surveillance systems shall be installed and operated only following prior review and written approval by the designated campus authority.

2. **Inventory and documentation**
   The designated campus authority shall maintain a master inventory and associated documentation of all existing and approved video and electronic surveillance systems, equipment, and authorizations.
3. **Management and operation**
   Video surveillance systems installation, administration, and management will be centralized (either university-wide or per-campus) and coordinated by the University Director for Public Safety, the campus Chief of Police, and the University Chief Security Officer. Exceptions to the centralized system(s) will be extremely rare, and only with prior approval of the designated campus authority and the University Chief Security Officer.
   Operators will be trained on the technical, legal, and ethical use of video and electronic surveillance systems and will perform their duties in accordance with this policy.
4. **Approval of operator access**
   The designated campus authority will review and approve requests for operator access to video and electronic surveillance systems.
5. **Storage and retention of surveillance information**
   Surveillance information must be stored in a secure location and configured to prevent unauthorized access, modification, duplication, or destruction. Surveillance information will be kept for no longer than sixty (60) days unless requested in writing by the Office of General Counsel or the campus Chancellor or Provost, and it shall be destroyed in a secure manner as soon as the retention period expires.
6. **Preservation of surveillance information**
   The Office of General Counsel or the campus Chancellor or Provost may request, in writing to the designated campus authority, that surveillance information be retained longer than sixty (60) days. The designated campus authority shall receive, document and store the written preservation request and ensure the preservation occurs in an efficient and effective manner.
7. **Release of surveillance information**
   Surveillance information shall only be released to non-operators under specific circumstances, and only upon review and approval of the designated campus authority and/or the Office of General Counsel, in consultation with the University Director for Public Safety, the University Chief Security Officer, and the University Chief Privacy Officer.
   The designated campus authority shall receive, document, and store each request for and approval of the release of surveillance information, and ensure that such requests are managed in an efficient and effective manner.
   Unauthorized access to, inadequate protection of, and inappropriate use, disclosure, and/or disposal of surveillance information must be reported immediately as outlined in "Information and Information Technology Incident Response Procedures".
8. **Use of surveillance information**
   Surveillance information may be accessed or otherwise used by authorized operators only as authorized and in accordance with this policy.
9. **Notice**
   Signs may accompany video and electronic surveillance systems. The designated campus authority, University Director for Public Safety, the campus Chief of Police, the University Chief Security Officer, and/or the University Chief Privacy Officer will determine when signs are appropriate. Any signage posted shall include a statement indicating that the surveillance is not actively monitored.
10. **Compliance Audit**
    The University Chief Security Officer or Internal Audit may audit the designated campus authority and surveillance operators for compliance with this policy.
11. **Consultation**
    The University Chief Security Officer, University Chief Privacy Officer, and/or the University Director for Public Safety are available to provide consultation or advice related to use of video and electronic surveillance systems.

Back to top

Definitions

Camera A digital or analog device that captures a single image (still, snapshot, photograph), a number of single images shot per time period (stop action, time lapse), or multiple images (motion, video). "Cameras" covers all image capturing devices, including but not limited to video cameras, cell phone cameras, webcams, and portable computing devices. Designated Campus Authority Individual or group responsible for reviewing and approving aspects of video and electronic surveillance systems. The campus Provost or Chancellor shall be initially assigned this duty, but this responsibility may be delegated to another senior campus official or appointed review committee that is not otherwise involved in the installation, operation, or monitoring of video and electronic surveillance systems. Electronic Surveillance Device A digital or analog device that has the capability to monitor or record audio, video, photographic images, or location data, including but not limited to cameras, microphones, audiocassette recorders, cell phones, webcams, and Global Positioning Systems (GPS). Facilities Buildings, grounds, and physical property that are owned or controlled - via leases or other contractual arrangements - by Indiana University, and whose operations are controlled by Indiana University. This definition includes but is not limited to, offices, labs, building exteriors, hallways, parking lots and garages, vehicles, busses, outdoor areas, and common areas. Buildings, grounds, or other properties owned by Indiana University, but whose operations are under the control and operation of a third party, shall not be considered facilities under this policy. Law Enforcement An electronic surveillance system used in the day-to-day prevention and investigation of violations of law. Examples of such systems include video cameras used in detective work, during interviews, and to record traffic stops. Operators Individuals who have been assigned responsibility by the designated campus authority for the installation, management, operation, and use of video and electronic surveillance systems. This includes but is not limited to computer system administrators, surveillance software administrators, surveillance installation technicians, and those who have access to surveillance information. Preservation The process of securely copying and/or storing surveillance information to prevent destruction and loss of materials. Surveillance Information All information captured by an electronic surveillance system. This definition includes system logs, audio, stills, snapshots, stop action, and video images whether transient, displayed, or recorded. Video The process of monitoring or recording visual images via stop action, time lapse, or motion cameras. Video and Electronic Surveillance Systems Any video or electronic surveillance system deployed by Indiana University, including its officers, administrators, employees, or agents, for purposes including, but not limited to, public safety, security, public

convenience, or operational effectiveness purposes. "Systems" may monitor or record a specific location or activity and covers all electronic surveillance devices, processes, technology, and equipment, including but not limited to microphones, cameras, images, audio, video, snapshots, configuration settings, logs, software, and hardware.

Back to top

Sanctions

Violations of university policies, including the failure to avoid a prohibited activity or obtain required approvals, will be dealt with in accordance with applicable university policies and procedures. Depending on the individual and circumstances, such sanctions could involve the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the General Counsel, and/or appropriate law enforcement agencies.

Failure to comply with university policies may result in sanctions relating to the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

Back to top

History

- Effective 1-Jan-2012
- Policy was updated in April, 2014 with minor changes to the definitions.