Video and Electronic Surveillance
PS-02

About This Policy

Effective Dates:
01-01-2012

Last Updated:
03-29-2022

Responsible University Administrator:
Executive Vice President for Finance and Administration

Policy Contact:
iupsadmn@iu.edu

Scope

1. Except as provided below, this policy applies to all video and electronic surveillance systems deployed by Indiana University, including devices, processes, technology, and equipment, that monitor or record Indiana University facilities, equipment, or grounds, and/or members of the university community using those facilities, equipment, or grounds ("Systems").

2. The following Systems are outside the scope of this policy:
   a. Systems used in health treatment settings, which are governed by the Health Insurance Portability and Accountability Act (HIPAA);
   b. Systems used for human subjects-based research, which are governed by federal law and in university policy RP-11-004, Research with Human Subjects;
   c. Systems deployed or used specifically for law enforcement purposes, which are overseen by the Chief of Police of each campus’ division of the Indiana University Police Department (IUPD) in accordance with "IUPD" General Orders.
   d. Systems used to observe, capture, or analyze Information Technology telecommunications traffic, which are governed by university policy IT-07, Privacy of Electronic Information and Information Technology Resources.
   e. Systems used to:
      1. deliver education;
      2. conduct teaching, non-human subjects-based research, or creative activity;
      3. conduct video conferencing;
      4. record public performances, events, or interviews;
      5. record practices or rehearsals, including athletics and performing arts;
      6. record news or press coverage;
      7. produce promotional materials;
      8. record and analyze video for parking enforcement purposes.
   f. Systems that are built into buses purchased for campus bus operations are subject only to PS-02.1 Procedures, Release of Surveillance Information, of this policy.

Although the Systems identified above are outside the scope of this policy, they may be subject to standards established by University Information Systems Officer (UISO) https://policies.iu.edu/policies/it-12-security-it-resources/index.html.
In the event any Systems identified above are to be used for any other purpose not specifically outside the scope of this policy, then this policy shall govern.

3. For further information about the types of Systems covered by the policy, see Related Information below.

Policy Statement

1. Indiana University respects the privacy of individuals who are using university facilities, equipment, or grounds. The university will take pragmatic and measured steps to provide an efficient, effective, safe, and secure environment for members of the university community, while avoiding unnecessary intrusions upon academic freedom or individual civil liberties including privacy, freedom of expression, and freedom of assembly.

2. The approval, installation, operation, and use of all video and electronic surveillance systems and devices 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.

3. Surveillance information obtained through video and electronic surveillance systems and devices shall not be accessed, used, or disclosed except as authorized in this policy.

Reason For Policy

The university may install and utilize Systems for the advancement and protection of public health, public safety, security, public convenience, and operational effectiveness.

Procedure

1. Approval, Installation, and Replacement of Video and Electronic Surveillance Systems
   a. Systems will be installed and operated only following prior review and written approval by Physical Security and Access ("PSA"), which is the individual or group within Indiana University Public Safety that is charged by the university with responsibility for reviewing and approving all aspects of video and electronic surveillance systems at all campuses.
   b. Requests for the installation of a new System or for updates to existing Systems must be submitted to PSA using electronic Form PS-02.4 Request for Surveillance Systems and Devices.
   c. Proposed System changes, i.e., changes in how surveillance information will be reviewed or used, changes in the nature of the physical space that impacts personal privacy, change in location or field of view of camera, etc., must be submitted for review and approval by PSA. (Form PS-02.4 Request for Surveillance Systems and Devices).
   d. Off Line and False Systems and Devices. Off line and false systems are prohibited. Systems that are off line, and/or for which no action to repair or replace can be shown, will be considered off line or false systems. It is the responsibility of the owner to remain in compliance with Policy PS-02 by removing false systems and devices.

2. Appropriate and Prohibited Uses of Video and Electronic Surveillance Systems
   a. 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, residential rooms, changing or dressing rooms, wellness rooms, clinical education rooms, and health treatment rooms.
   b. 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 identified by PSA and the processes identified in Procedure 1 above and have been completed.
   c. Systems shall not be used to conduct “routine surveillance” of employees or other individuals. PSA may consult with the unit and Indiana University Human Resources to ensure that requested Systems are installed and used in a manner consistent with IUHR policies.
   d. With the exception of spaces controlled by IUPD, Systems shall not be used to record audio.
e. System installation and operation shall be designed to avoid or minimize monitoring or recording of sensitive institutional or personal information which may be found, for example, on an individual’s workspace or other electronic displays.

f. Electronic tracking devices may be installed on university vehicles or other equipment or included in purchase specifications for vehicles or other equipment, for inventory management and deployment purposes. No purchase of an electronic tracking device will be processed by IU Purchasing until the unit wishing to purchase the device completes the processes identified in Procedure 1 above and receives approval for the purchase. For purposes of this policy, electronic tracking devices do not include mobile computing devices as defined by IT-12.1.

3. **Scope and Commissioning of Video and Electronic Surveillance Systems**
   a. As part of the authorization for a new or updated System, PSA will determine the scope of the System, which includes but is not limited to system selection, hardware selection, selection of hardware installation locations, and signage (if appropriate).
   b. PSA must review and approve the field of view for Systems installed for the purpose of capturing historical events (e.g., construction cameras, weather cameras). Field-of-view systems must comply with all requirements set forth in Procedure 1 above.

4. **Inventory and Documentation of Video and Electronic Surveillance Systems**
   PSA will maintain a central inventory and associated documentation of all video and electronic Systems and operator requests and decisions.

5. **Management and Operation of and Access to Video and Electronic Surveillance Systems**
   a. Systems installation, administration, and management will be centralized university-wide and coordinated by PSA. Exceptions to centralization will be extremely rare and will be made only with prior written approval of the Associate Vice President for Public Safety in consultation with PSA.
   b. Systems will be operated and accessed by a limited number of authorized operators who are trained on the appropriate use of these Systems. Requests for operator access to video and electronic surveillance systems must be submitted for review and approval to PSA using electronic Form PS-02.5 Request for Operator Access to Surveillance Systems. Operators shall:
      1. Limit access to the minimum amount of surveillance information needed to complete the task at hand.
      2. Never access surveillance information for personal profit or curiosity.
      3. Respect the confidentiality and privacy of individuals captured by the surveillance information.
      4. Share surveillance information only as allowed by Procedure 7 of this policy.
   c. Approved operators have access to view real-time surveillance information and access to up to 30 days of recorded surveillance information.
   d. Indiana University Public Safety may, on a case-by-case basis, authorize access to individuals who are not approved operators, but who need access based on their job responsibilities or in emergency situations. Proximity of other individuals to Systems while they are in operation does not constitute “access” within the meaning of this policy. Approved operators are responsible for all activity associated with their log-ins.

6. **Storage, Preservation, and Disposal of Surveillance Information**
   a. Surveillance information must be stored in a secure location and configured to prevent unauthorized access, modification, duplication, disposal, or destruction.
   b. With the exception of video proctoring information, surveillance information will be preserved no longer than 30 days unless pursuant to written preservation request. Video proctoring information will be stored for no longer than 365 days.
   c. Requests for preservation must be submitted to PSA using electronic Form PS-02.6 Request to Preserve Surveillance Information. Litigation holds and pending requests under the Indiana Access to Public Records Act (APRA) are common examples of preservation requests for surveillance information.
d. External requests from law enforcement may be submitted on requesting department's letterhead containing department ORI, requester's contact information, and reason for request.

e. PSA will retain the written preservation request and preserve the subject materials until the Office of the Vice President and General Counsel advises that the materials are no longer required to be preserved.

f. At the conclusion of any applicable preservation period, surveillance information shall be destroyed in a secure manner pursuant to UIOS standards.

7. Release of Surveillance Information

a. Requests for the release of surveillance information must be made using electronic Form PS-02.7 Request to Release Surveillance Information. Surveillance information will be released in accordance with IT-07.

b. External requests from law enforcement may be submitted on requesting department's letterhead containing department ORI, requesting officer's contact information, and reason for request.

c. PSA will document each request for and response to the release of surveillance information.

d. Unauthorized access to, inadequate protection of, and inappropriate use, disclosure, and/or disposal of surveillance information must be reported immediately in accordance with ISPP-26, Information and Information Technology Incident Response Procedures.

8. Compliance Audit

Operators, devices, and systems may be audited by Internal Audit or the Associate Vice President for Public Safety.

9. Consultation

The Associate Vice President for Public Safety and PSA are available to provide consultation or advice related to the acquisition, installation, and use of video and electronic surveillance devices and systems.

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.

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, buses, 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.

False and Off Line Systems and Devices: Surveillance systems and devices which are not connected to the network and/or for which no action to repair or replace has been initiated.

Members of the Indiana University Community: Any individual who is a student, staff, faculty member, university official, or any other individual employed by, or acting on behalf of, the university; other individuals while on Indiana University property, including employees of third-party vendors and contractors, volunteers, and visitors.

Law Enforcement Use: Use of any device or system by IUPD in the prevention or investigation of violations of law or in response to public safety concerns. Examples include, but are not limited to, body worn cameras, law enforcement in-car cameras, temporary deployable cameras, and cameras on unmanned vehicles.

Mobile Computing Device (IT-12.1): Includes electronic devices that are capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes laptop/notebook computers, personal digital assistants, smart phones, tablets; and other computing
and communications devices with network connectivity and the capability of periodically operating in different physical locations. Individuals who have been assigned responsibility 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.

**Operators:** Individuals who have been assigned responsibility by Physical Security and Access (PSA) for the installation, management, operation, and/or use of video and electronic surveillance devices and systems.

**Physical Security and Access (PSA):** Individual or group reporting to the Associate Vice President of Public Safety under the Executive Vice President for Finance and Administration. Individual or group responsible for reviewing, recommending, and rendering determinations on all aspects of video and electronic surveillance devices and systems.

**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.

**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. "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.

**Video:** The process of monitoring or recording visual images via stop action, time lapse, or motion cameras.

**Sanctions**

Violations of university policies, including the failure to avoid a prohibited activity or obtain required approvals, will be addressed in accordance with applicable university policies and procedures. Depending on the individual and circumstances, such sanctions could involve the IUHR or campus Human Resources, the campus chief official for academic affairs, the campus chief officer for student affairs, the Office of the Vice President and 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.

**History**

This policy was established on January 1, 2012, was updated in April 2014 with minor changes to the definitions, and substantively revised on December 16, 2021 and February 29, 2022.

**Related Information**

- PS-02 Video and Electronic Surveillance additional information (including PS-02.1 Procedures and PS-02.2 Frequently Asked Questions)
- Academic Policies
- Code of Student Rights, Responsibilities, and Conduct
- Indiana Voyeurism Statute
- Information and Information Technology Incident Response Procedures
- Policy IT-02: Misuse and Abuse of Information Technology Resources
- Office of Research Administration Compliance Services For information on conducting surveillance in health treatment settings (HIPAA) Institutional Review Board (IRB) For information on surveillance related to human subjects based research
- Policy IT-07: Privacy of Electronic Information and Information Technology Resources
Securely Removing Data | IU Information Security Office
Guidelines for Video Proctoring of Quizzes and Exams

Related Forms

PS-02.4 Form - Request for Surveillance Systems and Devices
PS-02.5 Form - Request for Operator Access to Surveillance Systems
PS-02.6 Form - Request to Preserve Surveillance Information
PS-02.7 Form - Request to Release Surveillance Information