

# Guidelines on Administrative Uses of Video Cameras

The utilization of video cameras for administrative purposes and the preservation of video recordings are increasingly useful in university operations. Iowa State University has adopted a policy ([Video Cameras, Administrative Uses](#)), which outlines responsibilities for protection of privacy and other legal standards.

Since 2003, Facilities Planning and Management (FP&M) Building Security Services has developed stringent standards with collaboration with the Department of Public Safety(DPS) on security related installations and management of security related systems. A single university security camera system benefits end users, DPS and the university by providing sophisticated, high end video recordings that are secure and reliable.

## Exempt Activities

These guidelines do not apply to the exempt activities stated in the “Exclusions” section of the “Video Cameras, Administrative Uses” as defined in the policy.

- Academic uses in teaching, research and extension;
- Police;
- Uses not intended to capture human activity;
- Recording athletic, ceremonial and performance events;
- Training programs;
- Use for journalistic purposes.

The respective units using video cameras for exempt activities set their own policies. Please consult with the unit for any policies governing those uses.

## Non-Exempt Administrative Uses

Administrative uses of video cameras are subject to the following requirements as indicated in the policy.

No Recording or Monitoring of Conversations: To comply with Iowa law prohibiting clandestine recording of conversations without consent, video camera equipment must be set to disable sound monitoring and recording unless protocols are set up and followed to collect the affirmative consent of each person whose voice communications are being monitored. Notice of sound monitoring or recording is not sufficient.

Retention Limited to 30 Days: Retention of recordings will be limited to 30 days, unless preservation is requested and approved under the Electronic Privacy policy. Because recordings can be used in ways to invade privacy or threaten safety, retention is limited. ISU policy does permit longer retention and access to such recordings, but only upon a showing of need, and approval by appropriate university administrators. See the [Electronic Privacy policy, Section 2.3, Investigations](#). Retention of single frames in a non-video format is excluded from this retention limitation.

Location of Cameras to Respect Privacy: Consideration must be given to camera placement to avoid invasion of privacy. Cameras should be aimed or set up so that use is limited to their intended purpose. For example a camera used for monitoring access to an outside doorway should be located and zoomed to serve that purpose, and not to broadly capture traffic down an indoor hallway. A camera installed to monitor customer waiting lines should to the extent possible avoid capturing employee or other activity. Cameras must avoid such areas where there is an expectation of privacy such as private offices, medical treatment areas, rest rooms, dressing rooms, locker rooms.

Approval for Permanent installation onto Buildings: To preserve the beauty of the campus and avoid damage to buildings or interference with building systems, permanent affixation to buildings requires authorization from the Office of the University Architect, which may specify that Facilities Planning and Management staff conduct the installation.

No Dummy Cameras: A dummy camera (i.e., a fake, simulated, or decoy camera) is a non-functional camera designed to mislead a person who sees it into believing the area is being watched or recorded. To avoid giving the public a false sense of security, use of dummy cameras is prohibited.

## Administration of Policy

Crime prevention and resolution uses (see section below) require prior review and approval by FP&M Building Security Services to assure integrity of the content and prevention of misuse of cameras and their recordings.

Other uses may not require pre-approval (see section below); however, units may choose to comply with the higher standards applied to crime prevention. Review of other uses by FP&M is recommended to assure proper application of the policy.

Contact FP&M Building Security Services at 294-4211 or [securitycameras@iastate.edu](mailto:securitycameras@iastate.edu) for determinations on permissible uses, and for advice on installation of cameras.

Per the [Video Cameras, Administrative Uses](#) policy, video recordings may be released in accordance with the [Electronic Privacy](#) policy, which requires approval at the senior vice president level.

## Additional Requirements for Certain Uses

The following uses require that the additional standards and processes below be followed.

ADMINISTRATIVE USE	REQUIREMENTS AND PROCEDURES
<p><b>Crime Prevention and Resolution</b></p>	<p><u>Applicability</u>: Cameras are installed primarily for securing premises, prevention of crime and resolution of suspected criminal behavior. This process may be used for other uses at the election of the unit installing the cameras.</p> <p><u>Requirements</u>:</p> <ol style="list-style-type: none"> <li>1. Equipment. Units must use cameras approved by FP&amp;M Building Security Services to assure compatibility.</li> <li>2. The requesting unit should be ready to demonstrate measures to limit use to the intended purposes.</li> <li>3. Notice of camera use must be prominently displayed</li> <li>4. Unit Staff. The unit requesting installation of the cameras must specify the individuals or the position(s) responsible for managing the camera. The unit must require staff to receive training from FP&amp;M in the following areas:               <ol style="list-style-type: none"> <li>a. Protection of privacy</li> <li>b. University data access policies</li> <li>c. Unit protocols to appropriately limit access to recorded content</li> </ol> </li> <li>5. Staff with access to recorded content must sign an appropriate acknowledgment of their duty to maintain confidentiality of the data.</li> <li>6. <b>NOTE REGARDING SYSTEMS INSTALLED OR PURCHASED PRIOR TO THE EFFECTIVE DATE OF THE POLICY</b>: All systems installed for crime prevention purposes must meet these requirements <b>as they are replaced</b> or by July 1, 2020, whichever comes first. Units that already have video cameras need to register them with FP&amp;M. See the Registration link above.</li> </ol>

ADMINISTRATIVE USE	REQUIREMENTS AND PROCEDURES
<b>Crime Prevention and Resolution (continued)</b>	<p><u>Procedure:</u> The requesting unit must complete an application an Administrative Video Camera Request at <a href="https://www.fpm.iastate.edu/buildingsecurity/new_surveillance_cameras.asp">https://www.fpm.iastate.edu/buildingsecurity/new_surveillance_cameras.asp</a> indicating how the unit will comply with the above requirements. The application will be reviewed and approved by DPS, UHR and FP&amp;M.</p> <p><u>Questions:</u> Contact FP&amp;M Building Security Services at 294-4211 or <a href="mailto:securitycameras@iastate.edu">securitycameras@iastate.edu</a>.</p> <p><u>FP&amp;M Building Security Website:</u> <a href="https://www.fpm.iastate.edu/buildingsecurity/new_surveillance_cameras.asp">https://www.fpm.iastate.edu/buildingsecurity/new_surveillance_cameras.asp</a></p>
<b>Customer Service, safety (non-crime) monitoring and similar uses (but not marketing use for public spaces and events)</b>	<p><u>Applicability:</u> This is a catch-all category for uses other than crime prevention or broadcast of public spaces and events. Typical uses are:</p> <ul style="list-style-type: none"> <li>• Monitoring for persons needing services, such as queues or reception or service desks</li> <li>• Monitoring the availability of equipment to assure efficient usage in a computer lab or similar setting</li> <li>• Monitoring use of equipment in a shop or laboratory to assure availability, proper use or safe use</li> </ul> <p><u>Requirements:</u></p> <ol style="list-style-type: none"> <li>1. Notice of camera use must be prominently displayed</li> <li>2. Personnel managing the camera and with access to recorded content must acknowledge responsibility to follow privacy protocols of the university and the unit, and sign an appropriate acknowledgement of that responsibility</li> <li>3. In cases where university personnel will be monitored on a regular basis, and where the monitoring occurs in a place that is not in a public area, or where the camera is set up with a view of the area not available from the public area approval must be secured from the vice president for University Human Resources (UHR) or designee. UHR shall monitor for privacy considerations and conduct any necessary discussion with employee representatives.</li> <li>4. <b>NOTE REGARDING SYSTEMS INSTALLED OR PURCHASED PRIOR TO THE EFFECTIVE DATE OF THE POLICY:</b> All systems installed for customer service, safety monitoring, or similar uses must comply with these requirements <b>as existing systems are replaced</b> or by July 1, 2016, whichever comes first.</li> </ol> <p><u>Questions:</u> Contact FP&amp;M Building Security Services at 294-4211 or <a href="mailto:securitycameras@iastate.edu">securitycameras@iastate.edu</a>.</p>

[Register your video camera / system here](#)