UTIA IT0303P – SECURITY CAMERA PROCEDURES

Effective: August 03, 2018
Last Reviewed: July 06, 2018 **Last Updated:** July 22, 2018

Objective:
The purpose of this document is to provide stipulations for the installation and use of any and all video surveillance equipment on property owned and/or operated by the University of Tennessee Institute of Agriculture (the Institute). The use of such video surveillance equipment (security camera) will be for the purpose of monitoring premises for vandalism, theft, or other safety measures as described in this plan.

Scope:
This document applies to security cameras installed and utilized at all non-Knoxville campus locations owned, operated, or provided by the Institute, as well as all students, faculty, staff, users, and visitors who access, use, or otherwise frequent these locations.

All Institute units, departments, and offices located on the Knoxville campus must go through the UT Police Department (UTPD) and their Surveillance Oversight Committee (SOC) for all requests. Only UTPD has the authority to select, coordinate, operate, manage, and monitor all campus video surveillance equipment for the Knoxville area campus locations.

Procedures:
Any County, Region, or AgResearch Center (office) interested in using any type of security camera must understand that the regional IT representative, OIT HelpDesk, or any other Institute IT representative will NOT be able to support the use and maintenance of any security camera. Should any office decide to purchase a camera after the initial consultation with the regional IT representative, that office will be responsible for maintaining and troubleshooting the camera on their own, or through the seller or the camera manufacturer.

The purpose of utilizing security cameras includes, but is not limited to:

- Protection of individuals, including faculty, staff, students, and visitors
- Protection of Institute-owned and Institute-operated properties, including but not limited to buildings and perimeters, entrances and exits, lobbies, hallways, offices, loading docks, storage areas, labs, and parking areas, by monitoring (real-time or otherwise) and recording of these areas
- Verification and use of access control systems
- Investigation of criminal activity, but only in conjunction with the appropriate law enforcement agency

Prior to purchasing and using any kind of security camera, the office must do the following:

- Contact the person responsible for management of the building if the office is in a location not owned by the Institute or University. Be sure to discuss:
  - Rules prohibiting cameras in a specific office location
  - Rules pertaining to the use of cameras
- Consult with the regional IT representative. This consultation is solely to:
  - Determine if the camera can be used in a location with an Ethernet connection
  - Determine if there would be potential problems with bandwidth, as no camera will be allowed on the wireless network if its use degrades actual WiFi performance needed by the entire staff for regular job responsibilities
- Notify the local law enforcement agency(s) of the plan to install a security camera. The following should be discussed:
  1. Where the camera(s) will be installed
  2. The appropriate contact if video recording shows any form of criminal activity
- Submit the following information to the Institute's Chief Information Security Officer (CISO):
  - A description of the purpose for the security camera
  - The number of cameras the office is planning to use
  - The location of the camera(s) to be installed
  - The names of those responsible for monitoring the camera(s)
    - These individuals should be selected on a need-to-know basis only
  - The frequency by which the recordings will be reviewed
    - Real time, daily, randomly, only when unusual activity has been suspected, etc.
  - The length of time the recordings will be kept
  - The location where recordings will be kept
  - Plans for keeping the storage locations secure
  - Plans for keeping the security camera and any related IT assets secure

<u>Requirements for Security Camera Use</u>

- Post signs notifying visitors that the premises are under surveillance and security cameras may be recording.
  - Hidden cameras will not be allowed.
  - Posting signs will not relieve an office of any liability for installing the security cameras if cameras are not allowed in an area of the premises.
- Disable the audio capability, as audio surveillance is not allowed without the consent of at least one person being monitored.
- If security camera is in a location where minors are staying (e.g., 4-H camps), written notification should be provided to the parents disclosing the use of cameras.
- Cameras shall never be placed in areas where privacy is reasonably expected, such as restrooms, dressing rooms, etc.

    - As stated in Tennessee Code Annotated, § 39-13-605, it is an offense to knowingly photograph, which includes video, "when the individual has a reasonable expectation of privacy, without the prior effective consent of the individual, or in the case of a minor, without the prior effective consent of the minor's parent or guardian…"
- Cameras shall never be placed in areas directly facing any Institute-owned IT asset classified as moderate, high, or business critical.
    - Cameras may be placed in these areas, but they cannot be focused directly on the screens of these IT assets.
- Any use of a security camera for purposes other than safety and security purposes as referenced in this policy is strictly prohibited.
- Individuals will not be monitored based on age, race, religion, gender, ethnicity, sexual orientation, disability, or any other discriminatory characteristic.
- The Director will contact the local law enforcement agency(s) immediately upon seeing unusual or suspicious activity.
- Employees are obligated to report good-faith concerns according to UT Policy HR0508 – *Code of Conduct*.
- Never store any video recordings unless there is a business need for such recordings, then delete as necessary, maintaining compliance with UT Policy FI0120 – *Records Management*.
- Recordings will be stored in a secure location with access limited to those responsible for maintaining the camera(s) and recordings.
- Recordings must not be tampered with or duplicated.
- Requests for disclosure or release of recordings must be submitted to UT Office of General Counsel and/or UT Media Relations.

References:

UTIA Glossary of Information Technology Terms
UT Policy HR0508 – *Code of Conduct*
UT Policy FI0120 – *Records Management*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)*
UT Knoxville Campus Procedures on the Acceptable Use of Video Surveillance Equipment
Tennessee Code Annotated, § 39-13-605

For more information, contact Sandy Lindsey, CISO, at (865) 974-7292, or email sandy@tennessee.edu.

Approval of Procedures

We approve UTIA IT0303P – *Security Cameras Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		08/03/2018
Charles Lambrecht	Computer Operations Manager, UTCVM		8/1/18
Brent Lamons	Director of Advising, Herbert College of Agriculture		7/26/18
Joel Lown	Coordinator, AgResearch		7/20/18
Emily Tipton	IT Coordinator, Extension		7/20/18
Kristy Keel-Blackmon	Communications Specialist, Forestry, Wildlife and Fisheries		7/20/18
Joanne Logan	Associate Professor, Biosystems Engineering and Soil Science		8/3/18