POLICY & PROCEDURE DOCUMENT

NUMBER: 5.5110

DIVISION: Information Technology

TITLE: Video Surveillance Systems

DATE: June 5, 2017

REVISED: _____

AUTHORIZED: Gordon Johnson, VP of Information Technology

I. Purpose and Scope

Western Kentucky University is committed to enhancing the quality of life of the campus community by integrating best practices of safety and security. This policy pertains to acceptable installation, operation and use of video surveillance technologies on WKU-owned or controlled property including areas in which affiliates operate (e.g. food services, building services). Adherence to this policy is mandatory and is necessary to ensure the protection of individual privacy rights in accordance with the University's core values along with local, state and federal laws. This policy sets forth the required and standardized procedures for the installation of video surveillance equipment along with the handling, viewing, retention, dissemination, and destruction of resulting data.

II. Policy

A. DEFINITIONS

Video Surveillance (VS): the combination of equipment and process that enables the real-time viewing or video recording of a physical space or location.

Video Surveillance Operator: Any person utilizing a video surveillance system typically but not limited to viewing live or recorded data.

Unit: A college, department, program, research center, or other entity utilizing the University's standardized video surveillance services as provided by the Information Technology Division. The services provided are typically custom per the unit's needs and established as a provider (WKU-IT) and client (Unit) relationship.

Physical Security Technologies Group: The operational group within the Information Technology Division responsible for the design, implementation, and ongoing maintenance of the University's standardized video surveillance system(s) on behalf of Units acting in a client capacity.

B. EXCEPTIONS

- Academic Application: This policy does not apply to academic use of video cameras for educational purposes. Examples include Lecture creation/capture & use of video recording as a research tool.
- Law Enforcement Surveillance: This policy does not apply to cameras used covertly by law enforcement for criminal surveillance during active investigations as approved by the WKU Chief of Police or other governing law enforcement agencies.
- Not related to Surveillance: This policy does not apply to still/video cameras or webcams unrelated to surveillance activity. Examples include construction cameras, WKU Public Affairs activities or recording of Athletics activities for post-game analysis, and video conferencing.
- Personally-owned Cameras: This policy does not apply to personally-owned still/video cameras owned and operated by members of the campus community and used for non-surveillance applications.

C. CONTACTS

Subject	Contact	Telephone
Policy Clarification and Interpretation	General Counsel	(270) 745-5398
Requesting to Install New or Replacement Video Surveillance Systems (VSS)	WKU Information Technology	(270) 745-7000
Support and Maintenance of University-standard VSS	WKU Information Technology	(270) 745-7000
Objecting to a VSS Installation	General Counsel	(270) 745-5398
Request a variance to implement a non-standard VSS	WKU Information Technology	(270) 745-7000
Subpoena or Other Legal Inquiries	General Counsel	(270) 745-5398

D. RESPONSIBILITIES

E. PRINCIPLES

1. All video surveillance installations must be part of the University's standardized system and approved through a formal process (see below), unless a variance is approved. Variances may be granted for unique situations which could include regulatory compliance concerns (ex. HIPAA) in which WKU Information Technology may exercise a first right of refusal.

2. All video surveillance system data must be viewable by the WKU Police Department unless a variance is approved. However, it is not inherently the responsibility of any other WKU entity to monitor another Unit's system. All Units are responsible for the appropriate use and monitoring of VS data associated with that Unit's coverage area.

3. Exterior cameras used for video surveillance are not to be utilized to look through residence hall windows, or to provide any better view of residential room interiors than unaided human vision from the same location.

4. Standard installations of WKU VS are not intended to be covert (hidden) but this policy does not prohibit the University Police Department or other law enforcement agencies having jurisdiction as part of an active investigation directly or through an agent, from authorizing legal engagement of surveillance systems covert or otherwise.

5. Video Surveillance Operators:

    a) Use of video surveillance technologies is confined to valid business, safety and security purposes and must be conducted in a manner that is professional, ethical, legal, and consistent with existing University regulations and policies. Any other unwarranted use of VS including but not limited to personal curiosity, eavesdropping, voyeurism, extortion or profiling based on a person's race, gender, sexual orientation, national origin, disability or other protected characteristic is strictly prohibited.

    b) Recording of any video surveillance system data, including audio, video, and metadata with a secondary device or application including but not limited to other video and still cameras, mobile phones, and screen capture software is strictly prohibited. Native exporting features of the VS Solution are not considered in this clause but are still subject to Release of Data restrictions.

6. Obtaining Approval

    a) The requesting unit's designated primary contact for this purpose, typically a Unit supervisor, must submit a formal request for these services via the IT Service Catalog http://www.wku.edu/it/contact. The WKU-IT Physical Security Technologies Group, in conjunction with other supporting groups, as needed, will be guided by the need for safety and security of people and property, concerns for the privacy of members of the university community, and the interests of these members to assembly and free speech.

    b) Video Surveillance installations may be approved in areas such as those:

        1) containing security mechanisms:
            a. Electronic access control systems, which monitor and record restricted-access at entrances to buildings and other areas.
            b. Alarmed areas, including intrusion/burglar alarms, exit-door controls, hold-up alarms, cashier locations, etc.
        2) containing sensitive files, data or operations.
        3) locations of the university grounds and buildings, including shopping areas, perimeters, entrances, exits, lobbies, corridors, common areas, receiving docks, and areas where no expectation of privacy exists.

4) housing sensitive operations, such as storage areas for special materials, laboratories, etc.
5) containing rare, high-value, or merchandise property including legal tender.
6) Other locations will be considered on a case by case basis in conjunction with WKU General Counsel.

7. Audio:

   Audio recording capabilities of video surveillance equipment will be disabled by the Physical Security Technologies Group upon installation unless otherwise authorized by General Counsel based on specific client use case.

8. Signage:

   a) Signage is not required in areas where there is no expectation of privacy. Though not required in such areas, a Unit may choose to display signage if they deem it to be a best practice for their situation. Signage must consist of approved verbiage and aesthetics. The Physical Security Technology Group can advise on this subject.

   b) Conversely if an area being covered by video surveillance is in an area where privacy is expected, as determined WKU General Council or applicable legal statute, then signage will be required.

   c) In locations where audio monitoring and/or recording is enabled, signage shall be displayed that clearly and specifically indicates that such capabilities are in place and may be in use. Signage must consist of approved verbiage and aesthetics. The Physical Security Technology Group can advise on this subject.

   d) The Unit must maintain appropriate signage if required by this policy or applicable laws. The Physical Security Technology Group can assist upon request.

9. Objecting to a video surveillance installation:

   a) An individual who believes the presence of a video surveillance system or component is in violation of this policy may file an objection with University General Counsel.

10. Storage, Retention, Release and Destruction of Recorded Material

    a) Generated video surveillance system data will be stored with physical and technological access restricted to authorized personnel only. The WKU-IT Physical Security Technology Group and supporting groups will to the best of their ability implement security best practices to safeguard this data.

    b) Generated video surveillance system data will be stored for the period of time selected by the Unit at the time of implementation or via a change request at a later date. The Physical Security Technology Group will make every attempt to meet the Unit's requests. Though implemented with several fault tolerant mechanisms, video data, due to volume, is not backed up using traditional means. In the unlikely event of catastrophic failure, data could be lost.

c) Data obtained through use of the surveillance system with a retention need exceeding the time selected by the Unit, must be exported and retained by the Unit. It is recommended to immediately export any data determined to be of specific value for the Unit's operations. Such retentions remain subject to this policy.

d) Release of recorded data must be approved:

    1) Units wishing to release data obtained from the video surveillance system must first seek permission from WKU Public Affairs or WKU Chief of Police

    2) All requests to the University for the release of data generated by a video surveillance system must follow the University's Open Records Request policy.

    3) Requests that take the form of subpoenas or other legal documents compelling production must be submitted to WKU General Counsel.

    4) Some Units utilizing these services are private business WKU Affiliates and are not subject to the same Open Records regulations as the University. Data generated by the Video Surveillance system for a non-WKU Unit is the property of said Unit and thus not necessarily subject to Open Records Requests.

e) Recordings or images used for prosecution of a crime shall be retained according to the relevant laws and rules of the court having jurisdiction unless directed otherwise by a court. The onus for retention in these cases is on the investigative entity.

11. Audit and Maintenance Requirements

a) The Unit shall conduct, annually at a minimum, audits that include review of approved operators and their access levels to video surveillance resources applicable to the unit.

b) The Unit shall immediately notify the Physical Security Technology Group of requests to add, modify, or remove user access. http://www.wku.edu/it/contact. Dedicated IT Service Catalog entries are available for these requests.

c) The Unit shall promptly notify Physical Security Technology Group of any change in the Unit's primary contact(s) for video surveillance change management.

d) The Unit shall promptly notify Physical Security Technology Group of any repairs or maintenance as needed.

12. Destruction or Tampering: Any person tampering with or destroying video surveillance system components may be subject to University disciplinary action and/or civil, or criminal action.

13. Miscellaneous

a) It is not recommended to grant students, student-workers, graduate assistants and like positions access to a video surveillance system.

b) These provisions may be overridden by court order or legislative actions.

14. Violation of Policy: Violations of this policy may result in University disciplinary action and/or civil or criminal action against the violator.

IV. Related Policies

See also:

- Open Records request. http://www.wku.edu/policies/