External Department End User Guide

for
DPS/UP-managed
Video Management System

Background

The Kennesaw State University Department of Public and University Police (DPS/UP) manages the video management system predominantly in use by the University for video surveillance cameras.

Video surveillance cameras are utilized primarily for:

- property protection related to deterrence of theft and/or other criminal behavior, protection of valuable resource(s)
- evidence / documentation potential related to property protection and access to valuable resource(s)
- extended responsibility related to academic integrity and/or laboratory safety
- hazardous materials monitoring and/or response

Purpose

The purpose of this end user guide is to provide parameters regarding the installation and use of video surveillance cameras connected to the video management system managed by the DPS/UP on University property, where such video surveillance cameras are not under the direct physical control of the DPS/UP (not within a building that is a DPS/UP facility) or otherwise designated as a 'Public Safety/University Police' camera.

Definitions

For the purposes of this end user guide, the below definitions apply:

Common area – An area which is available for use by more than one person. While an associated use restriction may reduce the total population having access to the area (such as a classroom, lounge, study room, interior hallway, lobby of a building closed to the public after hours, etc.), an individual's reasonable expectation of privacy is still greatly diminished. Exceptions are areas such as restrooms, locker rooms and dressing rooms, where such rooms may be used by more than one person at a time, but still have some reasonable expectation to some degree of privacy.

Crimes / Offenses -

> Murder/Non-Negligent Manslaughter: The willful (non-negligent) killing of one human being by another.

Negligent Manslaughter: The killing of another person through gross negligence.

Rape (a sex offense): The penetration, no matter how slight, of the vagina or anus with any body part or object, or oral penetration by a sex organ of another person, without consent of the victim.

Fondling (a sex offense): The touching of the private body parts of another person for the purposes of sexual gratification, without the consent of the victim, including instances where the victim is incapable of giving consent because of his/her age or because of his/her temporary or permanent mental incapacity.

Incest (a sex offense): Non-forcible sexual intercourse between persons who are related to each other within the degree wherein marriage is prohibited by law.

Statutory Rape (a sex offense): Non-forcible sexual intercourse with a person who is under the statutory age of consent. In Georgia, the statutory age of consent is sixteen (16) years of age.

Robbery: The taking or attempting to take anything from value of the care, custody, or control of a person or persons by force or threat of force or violence and/or by putting the victim in fear.

Aggravated Assault: An unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. This type of assault usually is accompanied by the use of a weapon or by means likely to produce death or great bodily harm.

Burglary: The unlawful entry of a structure to commit a felony or a theft.

Motor Vehicle Theft: The theft or attempted theft of a motor vehicle (all cases where automobiles are taken by persons not having lawful access, even though the vehicles are later abandoned - including joy riding).

Arson: Any willful or malicious burning or attempt to burn, with or without intent to defraud, a dwelling house, public building, motor vehicle or aircraft, or personal property of another kind.

Department - An organizational unit of the University, consisting of a grouping of personnel and management functions, and formally recognized as such; typically by designation as a ‘Department’, ‘School’, ‘College’, ‘Center’, ‘Institute’, or ‘Academy’.

Department head - The highest ranking administrator in a department within the University (e.g., Vice President, Assistant Vice President, Associate Vice President, Dean, Director, or department chair). The department head may designate at least one other person as a ‘department head designee’ to act in the department head’s capacity with regards to video surveillance cameras.

Department head designee - A full-time employee of the University who is in a supervisory or managerial position, and is designated by his or her department head to act on their behalf with respect to video surveillance cameras.

Departmental policy – A policy adopted by an individual department that is binding to the members of that individual department.

DPS/UP designated camera surveillance installation and maintenance vendor - One or more individuals or business entities that are:

- Identified through the State of Georgia Department of Administrative Services (DOAS) as being an authorized participant in a state contract for service; or,
- Identified through KSU Office of Fiscal Services as being an authorized participant in a University contract for service; and,
- Designated by the KSU Department of Public Safety and University Police as a vendor who can perform camera installations, repairs, warranty service and other services as a recognized distributor, retailer, installer and/or integrator of the video camera hardware and VMS currently in use.

Electronic file - A grouping of one or more bytes, utilizing a specific format, used to store and organize data. Video images captured by digital cameras are stored and organized within such electronic files.

Employee of the University - An individual who is employed by the University either on a part-time, full-time (regular or temporary) basis, or through other special employment situations.

End user - An individual who has been authorized to access and view video surveillance camera images and associated electronic files.

Enterprise or Auxiliary camera placement - A camera placement related to and/or requested by a department or unit that is understood to be an auxiliary enterprise, or auxiliary service, as defined by the Board of Regents' definition of such department or unit. This type of camera placement is associated with an activity that exists to provide a service directly or indirectly to students, faculty or staff, and for which a fee is charged that is related to, but not necessarily equal to, the cost of the service. Auxiliary enterprises are operated on a self-supporting basis, where the combination of fees and other revenues is sufficient to meet costs and, generally, are not subsidized by state appropriations, or other educational and general revenues. For the purposes of this guide, and absent a contrary categorical determination through BOR policy clarification, camera placements in the following departments and/or units are processed as being enterprise or auxiliary camera placements:

- Athletics
- College of Continuing and Professional Education
- Copy/Print Services
- Department of Student Activities
- Department of Sports and Recreation
- Housing and Residence Life
- K-Cash

- Parking and Transportation (except camera placements within parking lots and parking decks that are always open to and accessible by the public- these will be optionally managed by DPS/UP as University camera placements)
- Student Health Services
- Testing Center
- University Dining (Food Services)
- University Stores (Bookstores, Market, Owltec)
- Vending Services (vending machines)

File integrity - The accuracy, completeness, and validity of information in accordance with organizational values and expectations. For video files, ensuring that a file has not been altered in any unauthorized manner - that the image that was recorded remains unaltered after its creation, archiving, viewing and/or copying of the image.

File security - Ensuring that a file can be accessed only by those who are authorized to access it; and, that the risk of loss or corruption of data is minimized. For video files, that means that adequate login/password/authentication protocols are incorporated into the VMS software; and, that the method(s) utilized by the VMS software and associated hardware and network operations minimize the associated risk of data loss or corruption to the extent reasonably possible.

Formally adopted University policy - A policy that has been formally reviewed and approved by a University President.

Full-time employee of the University who is in a supervisory or managerial position - An employee of the University with full-time status, and who supervises one or more employees of the University and/or University-affiliated personnel; and/or, has managerial oversight of a University function or related process.

High danger area - An area associated with an increased level of danger to individual and/or collective life safety due to environmental factors. Examples include areas where potentially hazardous materials are stored or in use, areas where certain machinery is in operation, and areas where certain utility access/connections exist.

High security area - An area where there is a need to utilize one or more means of surveillance, security and/or protection elements due to its association with:

- Cash handling/monetary transaction points and/or associated storage locations - these are locations where potentially significant monetary transactions occur and/or money from such transactions is stored, as a primary function of the transaction points. Examples include ATMs, retail cash registers and Bursar customer service windows. Petty cash drawers and food vending machines are typically not considered cash handling/money transaction points and/or storage locations for purposes of this end user guide.
- Property of significant, tangible value - these are locations where the loss of an associated asset would affect the University in a financially adverse manner. Such property can be physical property, intellectual property and/or data, having an established valuation associated with the retention or loss of the property. Typically, while these assets are not as fungible as money, they may be transportable and not be secured to a building or other structure in such a manner as to make their removal unlikely.

- Critical infrastructure – these are assets, systems and/or network (physical or virtual) that the University considers so vital to it operations that their loss would have a long-term, debilitating effect on the ability of the University to deliver educational services and required support services to its customer base. Potential examples include communication networks and associated nodes, information/data storage locations, key utility (electricity, water, natural gas) transport and distribution points, operational command/control locations, logistical support/supply chain storage and distribution points (including the facilities that house any of the above), certain transportation system components and dams.
- Repository of financial information
- Repository of medical information
- Repository of educational information
- Repository of employment information
- Repository of proprietary, trade secret or similar confidential information that the University is required by law and/or agreement to safeguard
- Repository of information related to data maintained that contains personally identifiable information or sensitive personal information

Image - A two-dimensional constructed object that depicts a visual perception. For the purposes of video surveillance, such an image is typically a digital image (a numeric representation of digital values called picture elements- pixels) contained within and associated with one or more other electronic files.

KSU-owned or managed computer device - A computer (a device that can be instructed to carry out arbitrary sequences of arithmetic or logical operations automatically) purchased by, through or otherwise provided to an end user by the University. For purposes of this end user guide, the term computer includes desktops, laptops, notebooks, tablets and similar devices.

KSU-owned or managed network - A data network (a digital telecommunications network which allows nodes- data redistribution points or endpoints- to share resources) owned and/or managed by the University. Nodes are typically established over cable media such as wires or optic cables, or wireless media such as Wi-Fi. Commonly referred to as the ‘KSU network’.

Live monitoring - Viewing of live video feeds (and/or frames) from video cameras.

Private area - An area where an individual has a reasonable expectation of privacy. These areas generally have restricted access, are not used as common areas, and are clearly separated from public space and common areas. Often, one or more doors- capable of closing and being locked- is associated with this type of area. Examples are individual offices and toilet stalls. Exceptions would be locations that are considered high security areas and/or high danger areas.

Public convenience camera - Camera devices, typically attached to the network, for purposes of public convenience (to view, for example, construction project progress, weather conditions, or traffic conditions). These cameras must be placed in such a manner so that identifiable personal images are not transmitted. Such devices do not have storage capacity associated with them, since there is not an expectation that they will capture identifiable personal images for use in end user guide violations and/or criminal prosecution. Specific video surveillance camera manufacturer/models are designated by the KSU Department of Public Safety for various applications and environments.

Public space - a place that is generally open and accessible to people. This type of space, being open and accessible, tends to also be in public view- effectively eliminating, with few exceptions, any individual's reasonable expectation of privacy. Examples are roadways, parking lots, sidewalks, outdoor open space, and portions of buildings that are open to the public during certain hours. Exceptions are areas within places such as a public restroom.

Reasonable expectation of privacy - A concept based on: 1) an individual having an actual (subjective) expectation of privacy, and, 2) society in general recognizing that this expectation is (objectively) reasonable.

Record archive – Recording a copy of an existing, archived video feed (and/or frames) onto a file separate from the VMS file storage and file management software. Typically, this copy is made onto an end user's computer hard drive/internal storage and/or some type of external storage media, such as a DVD.

Remote access - Access to the VMS through a method other than using physical input to the computer upon which the VMS client software is installed. Typically, this involves using a VPN-type of software/service to access a computer remotely; or, may utilize a specific version of the VMS designed to provide VMS access in a remote and/or mobile environment.

Security camera – A video camera installed and utilized for the purpose of monitoring and recording cash handling/monetary transaction points and/or associated storage locations.

University-affiliated personnel - A non-paid individual (intern, volunteer, student assistant, research assistant, etc.) who is involved in and has ongoing responsibilities related to a KSU-sponsored program or activity, and is supervised by one or more KSU employees.

University camera placement - A camera placement related to and/or requested by a department or unit that is understood to be funded by state appropriations, or other educational and general revenues. For the purposes of this guide, and absent a contrary categorical determination through BOR policy clarification, University camera placements are those camera placements not determined to be enterprise or auxiliary camera placements.

Video camera - A camera used for electronic motion picture acquisition for security, surveillance, and/or monitoring purposes.

Video management system (VMS) - The software utilized by the KSU Department of Public Safety and University Police for the recording, processing and retention of video images captured by video surveillance cameras. The specific manufacture and software version is designated by the DPS/UP.

Video surveillance - The use of video cameras to monitor and/or record images and activity related to specific locations.

Video surveillance camera - Camera devices, typically attached to the network, for purposes of:

- Property protection related to deterrence of theft and/or other criminal behavior, protection of valuable resource(s)

- Evidence / documentation potential related to property protection and access to valuable resource(s)
- Extended responsibility related to academic integrity and/or laboratory safety
- Hazardous materials monitoring and/or response

Specific video surveillance camera manufacturer/models are designated by the DPS/UP for various applications and environments.

View archive - Viewing of video feeds (and/or frames) from archived files depicting past events and periods of time.

VMS access rights - Access privileges in the form of account provisioning and login information specific to the VMS client software that allows an end user to access and utilize the functions and features of the VMS client software.

VMS camera partitions and/or areas - Within the VMS, groupings of cameras and users into organizational sets. Partitions are used to specify which users and user groups have the ability to view a specific group of cameras; and, areas are used to organize the cameras into common groups for ease of use.

VMS client software - Software that allows an end user to access a service (processing and viewing of images) by a server by way of a network connection to the server. The specific manufacture and software version is designated by the DPS/UP.

General Use

Camera Systems, Equipment and Software

The currently approved equipment and software that may be utilized for video surveillance is available to requesting department heads and/or their designees upon request.

Unapproved or nonconforming devices will not be supported through or by the Department of Public Safety and University Police.

All equipment and/or software utilized for video surveillance, where the associated images and/or related electronic files are transmitted over any KSU-owned or managed network, and/or stored on KSU-owned or managed computer devices, must be reviewed by the University Information Security Officer (ISO) to determine if the associated electronic files are adequately preserved in accordance with BOR/USG policy.

Use of Video Surveillance

Video surveillance, in general, may only take place in public space, high security areas and/or high danger areas within buildings, exterior areas/entrances to buildings, parking lots and other common

areas. "Dummy" cameras that do not operate on a regular basis will not be installed or managed on behalf of a department by the Department of Public Safety and University Police.

Video surveillance will not be conducted in areas considered private in nature, such as:

- Staff and faculty individual offices (except where those areas are determined to be high value areas or high danger areas and the need for video surveillance is identified),
- Restrooms
- Locker rooms
- Residence hall living quarters
- Other areas that normally have a reasonable expectation of privacy.

This end user guide does not apply to:

- Use of cameras for law enforcement purposes and physical security operations as utilized by the Department of Public Safety and University Police.

- Hand-held mobile cameras, cell phones, webcams or other portable video cameras used for research, teaching, class work or personal use.

- Cameras, hand-held or otherwise, utilized as an instructional aid and/or to facilitate the delivery of instruction to remote locations, as well as enable video conferencing among remote sites.

- Web cameras for communication purposes used in auditoriums, conference rooms, faculty and staff private offices, and similar environments.

- Cameras, hand-held or otherwise, utilized by the University specifically for recording University-sponsored events, such as commencements, sporting events, promotional and other special events. The filming of public performances and events such as concerts, plays or athletic events is not covered by this end user guide, although other University policies may prohibit or restrict such recording.

- Cameras affixed to manned or unmanned aerial vehicles

- Cameras that are not operating on the video management system that is managed by the Department of Public Safety and University Police.

Use of Information for Official Purposes

End users will only utilize information acquired using the DPS/UP-managed video management system for official purposes.

Release of Related Information, Images and Records

Video images captured by video surveillance cameras are considered confidential, but may be subject to release under State or Federal law. Direct access to recorded images is limited to authorized end users and the Department of Public Safety and University Police. Release of recorded images outside of KSU is restricted to the Department of Public Safety and University Police.

Clery Reporting

End users of the video surveillance cameras, viewing any video recordings either as live monitoring or as view archive, are required to report the following to the KSU Police if discovered/viewed and believed by the end user to either be occurring or to have possibly occurred:

- Death of a person (For Clery purposes, this addresses: criminal homicide, including murder and non-negligent manslaughter and manslaughter by negligence)
- Sexual offense (for Clery purposes, this addresses: rape, fondling, incest and statutory rape)
- Robbery
- Aggravated assault
- Burglary
- Motor vehicle theft
- Arson

It is not the responsibility of an end user to search archival video for these types of incidents, or determine if one of the above incidents did in fact occur, or initiate making a copy of any related archival video to try to document such incidents. The end user must simply notify KSU Police if they happen to view an activity or event that they believe may be related to one of the above listed types of incidents.

FERPA

Any recording that includes personally-identifiable images of students has the potential to be treated as an education record in accordance with the Family Education Right to Privacy Act (FERPA).

Audio Recording Capabilities and Use

The Department of Public Safety and University Police must approve placement of video surveillance cameras with audio recording capabilities, and their subsequent use.

Signage

Department heads utilizing video surveillance within their areas of responsibility are encouraged to prominently place signs informing persons they may be subject to video surveillance or monitoring. Signs should be located in plain view for all faculty, staff, students and guests to see. The wording on

the signs should not create a false sense of security to lead someone to believe that the cameras are being monitored live if they are not.

If audio recording via one or more video surveillance cameras is utilized, signs must be prominently placed informing persons that they may be subject to video and audio monitoring. Signs should be located in plain view for all faculty, staff, students and guests to see. The wording on the signs should not create a false sense of security to lead someone to believe that the cameras are being monitored live if they are not.

Installation

A department head, pending available funding, may request and authorize the installation of a video surveillance camera, or a public convenience camera, for a location that is owned or leased by the University and under the department head's area of responsibility. Funding for the video surveillance camera, camera installation, associated network connectivity provision, required storage space for video images, licensing, annual service maintenance agreement, repairs, replacement and other associated costs will be the responsibility of the requesting department.

Each request will be evaluated by the DPS/UP to determine if the request is:

1) congruent with the intended use of the video surveillance camera or public convenience camera in accordance with this end user guide; and,
2) use of one or more surveillance cameras associated with the requested location is not contrary to other formally adopted DPS/UP policies, formally adopted University polices, or, would unreasonably impact University operations.

The DPS/UP may also consider, on a case-by-case basis, if justification for the request exists based on one or more of the following factors:

- asset value protection;
- functional criticality of the asset or assets being surveilled;
- validation of any described association with a legal requirement, regulatory requirement, and/or adopted University standard;
- historical incidents of crime, policy violations, code of conduct violations and/or safety incidents related to the location or type of location.

The review process will incorporate a recommendation to the Chief of Police or his/her designee, who will approve, disapprove or modify the request. The requesting department head will be notified of the DPS/UP decision. Any proposed modification will be submitted back to the requesting department head for review, and if accepted by the requesting department head, will move forward in the process as an approved request.

A requesting department head may appeal a decision by DPS/UP to disapprove a video surveillance camera installation by submitting an appeal request, in writing, to the Chief of Police. The requesting department head will be notified of the decision reached by the Chief of Police. If a request is approved, the request is processed for a site evaluation and quote request. Any proposed

modification will be submitted back to the requesting department head for review, and if accepted by the requesting department head, will move forward in the process as an approved request.

A “Video Surveillance Camera Installation Request Form” can be found on the DPS/UP website.

Site Evaluation

The following Prerequisites must be met before a video surveillance camera installation quote can be generated:

1. There must be identifiable access to the KSU network. If no pathway to the KSU network can be identified within the site (example: no network switch or network connectivity), the requesting department head will be referred to contact UITS via the UITS service desk to establish a KSU network access point before the video surveillance camera installation process can continue.

2. If there is existing KSU network access, there must be sufficient network switch capacity to accept the number of device inputs required for the requested video surveillance camera(s). If sufficient capacity does not exist, the requesting department head will be referred to contact UITS via the UITS service desk for additional network switch capacity before the video surveillance camera installation process can continue.

3. If neither of the above pre-requisites can be met, wireless connectivity options will be evaluated with the designated camera surveillance installation and maintenance vendor, UITS, DPS/UP and the requesting department head prior to any continuation with the installation process.

4. Mounting a camera onto a building’s exterior wall, and/or any penetration of a building’s exterior wall or roof for cabling (other than the use of an existing channel/conduit) requires approval by Facilities prior to installation.

5. Any excavations, including trenching and boring, requires approval from Facilities prior to installation.

6. Exact video camera placement will be determined through desired viewing area, available placement locations (walls, ceiling, mount/housing requirement, etc.), and network accessibility.

Quotes

For University camera placements, a purchase and installation quote will be generated through DPS/UP personnel, including any associated equipment costs, software licensing costs, server storage space costs, network cabling costs, and routing through applicable UITS technology purchase approval process, and supplied to the requesting department head and/or department head designee. Once the quotes have been processed and one or more purchase orders issued, DPS/UP will coordinate the installation and initial testing of the new video surveillance camera(s).

For Enterprise and/or Auxiliary camera placements, a purchase and installation quote will be generated through a DPS/UP-designated vendor and supplied to the requesting department head and/or department head designee. The designated vendor will furnish DPS/UP floorplan and/or elevation drawings of proposed camera locations and required network cable termination points in order to request network cabling installation, server storage space quotes, and technology purchase approval from UITS on behalf of the requesting department. The designated vendor will liaison directly with UITS on network cabling installation if the designated vendor will also be installing any applicable network cabling. Once the quotes (cabling, server/storage, equipment purchase, applicable VMS software licensing and installation) have been processed and one or more purchase orders issued, the designated vendor will coordinate the installation and initial testing of the new video surveillance camera(s).

Provisioning

The requesting department head may authorize access to the VMS as follows:

1) University-affiliated personnel: access the VMS for live monitoring of the video images produced by one or more cameras within one or more VMS camera partitions and/or areas that are either associated with that department head's area of responsibility, or are other VMS camera partitions and/or areas that have been designated for community access/viewing.

2) Employee of the University: access the VMS for live monitoring and/or view archive of the video images produced by one or more cameras within one or more VMS camera partitions and/or areas that are either associated with that department head's area of responsibility, or are other VMS camera partitions and/or areas that have been designated for community access/viewing.

3) Full-time employee of the University who is in a supervisory or managerial position: access the VMS for live monitoring and/or view archive and/or record (make copies of) archived video images produced by one or more cameras within one or more VMS camera partitions and/or areas that are either associated with that department head's area of responsibility, or are other VMS camera partitions and/or areas that have been designated for community access/viewing.

It is the responsibility of the requesting department head to provide oversight regarding the use of the video surveillance system by those personnel the requesting department head has designated for such access and use; and, to update their authorization to access the VMS as the status of authorized personnel change (i.e. transfer, change in job responsibilities, separation from employment, etc.).

Personnel who are authorized by a department head will receive:

- Login credentials for the VMS
- User manual

- VMS client software use orientation

A “VMS Access Authorization Form” will be provided to the requesting department head and/or their designee at the time of provisioning, and will be reviewed for renewal annually by DPS/UP personnel.

Client Software Application

The requesting department head may authorize a VMS client installation on one or more KSU-owned or managed devices, so that authorized University-affiliated personnel can utilize assigned credentials to access the VMS. VMS client software application will not be installed on any device not owned or managed by KSU, the University System of Georgia or the Board of Regents.

Remote access to the VMS software, camera system components, and/or the VMS server(s) outside of the provisioned VMS features and functions, will only be accomplished through an approved virtual private network (VPN) and an associated process identified and approved by the University ISO.

It is the responsibility of the requesting department head to initiate the removal of the VMS client software from a designated KSU-owned or managed device when such software is no longer necessary to have installed on the device.

The DPS/UP will, on an annual basis, review identified VMS client software installations, and verify status with their authorizing department head.

A “VMS Software Install/Uninstall Request Form” will be provided to the requesting department head at the time of provisioning, and will be reviewed for renewal annually.

Retention of Video Image Data

Digital images are retained by KSU as follows (default):

- Security cameras (locations where cash handling/monetary transaction points and/or associated storage is a primary function): minimum of 30 days
- All other cameras: minimum of 12 days

After these periods, digital images on any sever or similar computer hardware (that has not been archived onto separate storage media, such as a DVD) may be recorded over or deleted. However, pending available funding, if a longer retention period is required, a department head can request longer retention periods for cameras within one or more VMS camera partitions and/or areas that are associated with that department head’s area of responsibility.

Department heads can, pending available funding, elect to utilize cloud-based storage instead of or in addition to KSU-maintained storage. Availability and cost is dependent on VMS feature use, file storage volume and/or retention period.

Operations and Maintenance

After installation and initial provisioning, the Department of Public Safety and University Police will provide the following systemic support:

- VMS software patches and version updates
- Firmware updates to all approved (brand/model) cameras that are part of the VMS
- Coordination with UITS regarding server updates, server replacements, and server operating system patches and updates
- Coordination with UITS regarding KSU network outages, network maintenance, and network connectivity / function repair and restoration
- Beyond basic troubleshooting assistance, coordination of warranty camera replacements, non-warranty camera replacements, warranty repair work and non-warranty repair work with a DPS/UP-designated vendor for cameras identified as University placements, in accordance with available DPS/UP staff resources
- Beyond basic troubleshooting assistance, referral to a DPS/UP-designated vendor for warranty camera replacements, non-warranty camera replacements, warranty repair work and non-warranty repair work for cameras identified as Enterprise or Auxiliary placements

After installation and initial provisioning, the requesting department head (or their designee) is responsible for:

- Routinely checking the functionality of all cameras within one or more VMS camera partitions and/or areas that are associated with a department
- Contacting DPS/UP personnel for initial troubleshooting of functionality
- Allocating funding for camera replacement and repair work with the DPS/UP-designated vendor as needed, either in coordination with DPS/UP or through a resulting referral by DPS/UP. Associated activities include, but may not be limited to, obtaining quotes from one or more DPS/UP-designated vendors, processing purchase order requisitions in compliance with KSU/BOR procurement policy and rules, as required, and scheduling service appointments to ensure vendor access to facilities and camera installation sites
- When not funded through annually designated institutional funding, service maintenance agreement (SMA) costs associated with the cameras within one or more VMS camera partitions and/or areas that are associated with a department
- When not funded through annually designated institutional funding, server replacement costs and network infrastructure replacement costs (as identified and/or required by UITS) associated with the cameras within one or more VMS camera partitions and/or areas that are associated with a department

Video Surveillance Camera End of Support Notices and Unsupported Video Surveillance Cameras

In the event that the VMS does not support, or ceases to provide support for, a specific video surveillance camera make or model in use within the university due to the age of the camera or unresolved hardware and/or firmware security issues, notice will be made to applicable department heads (or their designees) who have applicable surveillance or public convenience cameras located in their respective partitions/areas of their responsibility regarding the last date that the video

surveillance camera will be provisioned for service within the VMS. The department head may elect to replace the affected cameras or have them removed:

Replacement of Unsupported Video Surveillance Cameras

When replacing an existing video surveillance camera, the process depicted in the 'installation' section of this end user guide will be applicable.

Removal of Unsupported Video Surveillance Cameras

DPS/UP personnel may be able to remove unsupported cameras (depending on location, mounting height, physical access to camera and/or availability of Facilities support as needed) associated with University placements. For University placements that DPS/UP personnel are unable to remove, and for all Enterprise or Auxiliary placements, the requesting department is responsible for any costs associated with a removal of a camera by non-DPS/UP personnel and/or third-party vendor(s); as well as any costs associated with structural, cosmetic repairs, or restorations (examples: replacement of ceiling tiles, wall patch/paint, removal of network cable- if required by UITS).

Video Surveillance Camera Projected End of Life / Life Cycle Replacement Estimates

End of life for video surveillance cameras typically arrive as a result of:

- The manufacture no longer makes replacement parts for the particular model of camera in use
- The labor costs and/or cost of repairing a particular camera in use, when compared to replacing the camera with a new, working model, makes the repair option appear to be cost prohibitive

In instances where video surveillance cameras in use appear; based on camera age, observed condition of camera(s), known maintenance issues and/or manufacturer notices: near, at, or past their expected life expectancy, DPS/UP personnel will notify potentially affected department heads (or their designees) of the circumstances so that they can consider options related to camera replacement or removal in future budget cycles and funding allocations.

Adherence to Guides

Failure to follow the parameters outlined in this guide could lead to suspension of camera VMS access to end users by the Department of Public Safety and University Police.

Associated Policies/Regulations for Reference

a. BOR Information Security End user guide: 11.3.1
b. BOR USG Records Retention Schedule: 0472-13-029A
c. BOR USG Policy 7.2.1
d. BOR USG Policy 7.2.2
e. KSU Network Access End user guide
f. KSU Enterprise Information End user guide
g. KSU Data Security End user guide
h. KSU User Accounts and Password End user guide
i. O.C.G.A. § 16-5-1: Murder, malice murder, felony murder, murder in the second degree
j. O.C.G.A. § 16-5-2: Voluntary manslaughter
k. O.C.G.A. § 16-5-3: Involuntary manslaughter
l. O.C.G.A. § 16-6-1: Rape
m. O.C.G.A. § 16-6-2: Sodomy, aggravated sodomy
n. O.C.G.A. § 16-6-22.1: Sexual battery

o. O.C.G.A. § 16-6-22.2 Aggravated sexual battery
p. O.C.G.A. § 16-6-22: Incest
q. O.C.G.A. § 16-6-3: Statutory rape
r. O.C.G.A. § 16-8-40: Robbery
s. O.C.G.A. § 16-8-41: Armed robbery
t. O.C.G.A. § 16-5-21: Aggravated assault
u. O.C.G.A. § 16-5-24: Aggravated battery
v. O.C.G.A. § 16-7-1: Burglary
w. O.C.G.A. § 16-7-2: Smash and grab burglary
x. O.C.G.A. § 16-8-2: Theft by taking (as applied to motor vehicle theft)
y. O.C.G.A. § 16-7-60: Arson in the first degree
z. O.C.G.A. § 16-7-61: Arson in the second degree
aa. O.C.G.A. § 16-7-62: Arson in the third degree
bb. The Family Educational Rights and Privacy Act (FERPA): 20 U.S.C. § 1232g; 34 CFR Part 99
cc. The Clery Act: 20 U.S.C. § 1092(f)