EPOKA UNIVERSITY

Guideline on the Functioning of the CCTV system

Table of Contents

1. ABBREVIATIONS

CCTV	Closed Circuit Television
IT	Information Technology
PTZ	Pan Tilt and Zoom
DVR	Digital Video Recorder
CDROM	Compact Disc Read Only Memory
DVD	Digital Versatile Disc
IMP	Information Management Programme
NVR	Network Video Recorder
VMS	Video Management System
RI	Register of the Incident
SARs	Subject Access Requests
ICTC Office	Information and Communication Technologies Coordinating Office

2. DEFINITIONS

University: Epoka University

Security Controller: is any natural or legal person appointed by the Rector of the University. His/her responsibilities are:

- to hold, process, manage, archive and control personal data;
- to ensure that the registration is completed;
- to ensure that the entrance and the control room is under surveillance of the cameras;
- to document training records for each authorized CCTV operator to be maintained.

Security Supervisor: is the head of the security services staff appointed by the Security Controller. His/her responsibilities are:

- to supervise security services staff;
- to prepare and maintain shift work schedules;
- to review and conduct thorough incident investigations;
- to train security staff, and assist in operational policy development;
- to ensure that any forms mentioned in this guideline are available to Security Services staff as required;
- to be responsible for the operation of the CCTV equipment;
- to ensure no unauthorized or inappropriate use is made of the system;
- to be responsible for production of any images to be retained for evidential purposes;

- to carry out a weekly check of paperwork to ensure all procedures are being complied with;
- to authorize for the removal of tapes or other recorded media from the University control;
- to be responsible for any amendments to the associated forms;
- to ensure that regular audits are conducted into the operation of the system;
- to conduct an annual evaluation on the functioning of the system and equipments and formally report to the Security Controller of Epoka University.

Security Services Staff: are proposed by the Security Supervisor and appointed by the Security Controller.

His/her responsibilities are:

- to fully ensure the implementation of the Guideline, all site security requirements and duty assignments contained in the Guideline;
- to be fully conversant with the layout of the area he/she monitors and be aware of the current threats and challenges faced by the institution;
- to monitor the live CCTV camera outputs within the scope of Guideline;
- to identify suspicious and criminal events and to ensure an effective guarding response;
- to be fully conversant with the principles of "Lock Down – Evacuate – Place of Safety" relating to internal protection of University staff and visitors during a terrorist event in the vicinity;
- to be fully conversant with emergency evacuation/controlled movement, internally to a place of safety procedures at all the buildings that are monitored;
- to contact by telephone the police regarding images captured on the CCTV system for the purposes of security or the prevention or detection of crime;
- to register in the Daily Register of the Incidents any suspicious activities or incidents monitored and recorded by CCTV equipment during his/her shift. The date, time, location, camera number, scope of the storing, and type of incident, are to be noted for possible investigation.

3. PURPOSE OF THE CCTV SYSTEM

The purpose of the University CCTV System on the Campus is to provide staff, students and visitors with a physical surveillance system that will enhance safety, security and the prevention and detection of crime. This document refers to the systems operated and controlled by the University's ICTC Office and Administrative and Technical Affairs Office.

4. SYSTEM DESCRIPTION

For the purpose of this Guideline, CCTV equipment includes cameras, transmission, and monitoring and retrieval equipment as defined in **Annex I**.

CCTV services operate a number of "streetscape" cameras covering the main entrance of the Epoka Campus and all the perimeter of the campus.

There are further cameras within university buildings monitoring both public and secure areas. Most of these cameras are static, although there are fully functional cameras in strategic locations.

All the cameras are centrally controlled and monitored at Server Room located at A-Building. There is a secondary monitoring center at the office of ICTC Office located at E-Building. One virtual machine is used to record video for A- Building, one virtual machine is used to record video for Perimeter and Main Entrance area. Two virtual machines are used to record video for E-Building and one virtual machine is used to record video from Dormitory.

This Guideline applies to all CCTV equipment operated by ICTC Office and Administrative and Technical Affairs Office at the above locations.

5. CONTROL ROOM OPERATION

The system shall be operated and maintained in accordance with this Guideline. A paper copy of this Guideline is located at the CCTV control desk for reference purposes.

All operating staff are to be fully conversant with the provisions and Operating Instructions for the Control Equipment as outlined in this Guideline.

It is the responsibility of the Security Supervisor to ensure that any forms mentioned in this policy are available to Security Services staff as required.

5.1 Access to Control Room

Access to control rooms is strictly controlled. All persons other than security staff entering the control room are required to complete the personal data registration regarding the person, time and reason why they had reason to gain access to the control room. It is the responsibility of the Security Controller to ensure that the registration is completed. The entrance and the control room

is under surveillance of the cameras.

5.2 Staff Verification

All security staff who have access to the CCTV control equipment shall posses a Certificate on the conduct of Training necessary for the purposes of operating the CCTV system and Confidentiality Declaration carried out.

5.3 Authorized Operation of CCTV Equipment

The Security Supervisor is the person responsible for the operation of the CCTV equipment and for ensuring no unauthorized or inappropriate use is made of the system.

The use of the system is to be restricted to the intended purpose of the system as outlined in Section 3. Use of the system outside the defined scope may constitute a criminal act. Only persons who have received full training on the operation and use of the CCTV equipment shall be authorized to operate the equipment.

Persons operating the system will not use the cameras to focus through windows of University premises unless acting under specific instructions of the Security Supervisor. Those instructions will only be issued in the event of an incident or threat to safety and security.

Suspicious activities or incidents monitored and recorded by CCTV equipment shall be registered by the operator in the Daily Register of the Incidents. The date, time, location, camera number, scope of the storing, and type of incident, are to be noted for possible investigation.

If a request is made by the police or other public body to conduct covert surveillance using the University's CCTV system, written authorization is required under the legal framework of Albanian Legislation. Authorities have no power to target individuals inside residences or motor vehicles. Breach of privacy is a criminal offence. All requests of this nature are to be recorded on a Request for Observation Record sheet.

5.4 Training

All operators require undergoing a programme of training on the system operation including relevant health and safety requirements. Documented training records for each authorized CCTV operator shall be maintained by the Security Controller.

5.5 Liaison with the Police

Suspicious activities or incidents if noted are to be brought to the attention of Police via telephone.

5.6 Processing of Images

According to Directive No. 3, dated 05.03.2010 of the Commissioner on the Protection of Personal Data on "Processing of Personal Data with Video Surveillance System in Buildings and other Environments" personal data must not be retained for longer than is necessary for the

purpose for which they have been collected. In this context, CCTV data are kept up to 60 days. After this date, the data are deleted or destroyed, except cases for the purpose of providing evidence for the police investigation.

The DVR units are programmed to automatically delete any recorded video files which are older than five days the cameras around the perimeter of the campus and 13 days the cameras inside the buildings.

Any images retained (on CDROM or DVD) to be used as evidence are kept securely within the Security Supervisors office. The Security Supervisors are responsible for production of any images to be retained for evidential purposes. Any such images will be retained only for as long as required by the Directive No. 3, dated 05.03.2010 of the Commissioner on the Protection of Personal Data (for the purpose of providing evidence) and will then is destroyed.

Access to the DVRs is limited to access at the DVR units themselves or authorized workstations, and only then to persons who have correct levels of access. The DVRs are all only accessible to persons having correct login identification and password. The DVRs and their associated monitors are all located in rooms away from the general public where private viewing can be facilitated.

5.6.1 Recording of Images and Production of Still/Video Images

With the advent of digital recording media, the transportation and multiple copying of video images is very much simpler. It also means images can be transported across the world instantly as email attachments/uploads to websites etc. It is very important that the risk which this presents to individual privacy is recognized and appropriate steps taken to prevent unauthorized access to the recordings. With this in mind, it is expressly forbidden to make or take any recordings from the CCTV digital recording systems without proper cause.

Where digital video evidence is to be used by the Police or other law enforcement authority (see Section 6.1), an entry will be made into the Register of the Incident (RI), which details what has been recorded and when this was done. It will also record the Supervisor who carried out the recording, verification and watermarking and the police officer whom the recording was handed to. When a recording of images from the DVR is made, the location of all copies of the file are to be noted in the "Recording Record Sheet", the location of all copies of recording must be constantly known and recorded.

The CDROM or DVD which is handed to the Police will be marked with the RI record number, in permanent felt pen, to help tracking of the recording. All the copies of footage recorded from the CCTV system onto either in a PC, CDROM or DVD are to be recorded in the RI against the production record. Each disc is to be given an individual number. All recorded images (static or motion) removed (i.e. images saved onto another system or media) from the digital recorders must be recorded in the "RI" and "Video Record Sheet". Additionally all activity on the DVR units is automatically logged on the unit.

5.6.2 Viewing of Recorded Images

Only authorized persons will be permitted to view recorded images. This may include an officer from an authorized law enforcement agency, such as the police. The viewing of recorded images is only to be carried out in connection with the purposes defined in section 4 of the Directive No. 3, dated 05.03.2010 of the Commissioner on the Protection of Personal Data on "Processing of Personal Data with Video Surveillance System in Buildings and other Environments". Any use outside the defined purposes is a breach of the Data Protection Law.

Recorded images must only be viewed in places where unauthorized persons cannot see the images.

Each time a DVR is accessed, user identification and password must be entered. All actions on the DVR units are logged against the login ID. This helps ensure that there is an auditable trail.

Where an authorized person is viewing images, this is to be recorded in the "Third Party Viewing Record".

The reviewing of recorded images is documented on the "Internal Viewing Record". This is used where authorized persons within the University are reviewing footage. Where third parties, external to the University, are reviewing the footage the "Third Party Viewing Record" shall be used. If the images are stored on CDROM or DVD for evidence purposes, this would be recorded on the "Productions Record Form".

5.6.3 Removal of Video Tapes / DVDs

Removal of tapes or other recorded media from under University control requires to be authorized by the Security Supervisor clearly recorded on 1) Individual Tape Record Sheet, 2) RI and 2) Production Record Form.

When tapes/CDROMs/DVDs have completed their life cycle they are to be logged out of the system and destroyed. A confirmation of destruction is to be obtained and displayed with the Individual Tape Record Sheet.

All the digital recorders are configured to ensure that video is not stored for longer than the defined up to 60 days.

5.7 Care of Digital Recording Systems

Digital video recorders are to have a diagnostic check carried out by the CCTV maintenance company as part of the routine quarterly maintenance. This should include system health, software patch status and hard disc capacity and reliability.
All digital video recorders (DVR) are to have any software patches realized by the manufacturer applied as soon as possible.
All digital video recorders are to be connected within a secure internal part of the university network and should not be available to persons outside the university. All DVRs must be held within a secure place, and must be password protected to prevent unauthorized access to the system, software or recordings.

6. REQUEST PROCEDURES

- Requests by students regarding the control of the CCTV system shall be submitted to the Dean of Students Office. After evaluating the request, the Dean of Students Office shall forward the request to the Security Controller for the final decision on the matter to be taken.

- Requests by staff and third parties regarding the control of the CCTV system shall be submitted to the Security Controller who after conducting the necessary evaluation shall take the final decision on the matter.

7. DATA PROTECTION

Under the Law No. 9887, dated 10.03.2008 "On the Protection of Personal Data", personal data includes any image from which an individual may be identified. The processing of personal data includes the recording, viewing, storage and destruction of personal data. The University is responsible for all CCTV owned and operated by the University and is the data controller for the requirements of the Law No. 9887, dated 10.03.2008 "On the Protection of Personal Data".

7.1 Disclosure to Third Parties

Disclosure of recorded images to third parties will be controlled and consistent with the purpose for which the system was established. Any requests for images and subsequent disclosures e.g. by police, should be recorded and a record retained by Security Services staff in accordance with section 5.6.2.

If police or other law enforcement agencies approach the University wishing to have access to images captured on the University's CCTV system, they must provide a standard Personal Data Request Form, in accordance with the relevant guidance issued by the Directorate of the State Policy of Albania.

The form should state clearly what information is requested and the purpose of obtaining the information i.e. required for an investigation concerning the apprehension or prosecution of offenders, and it must be signed by the investigating officer and counter-signed by an officer of a senior rank.

Where the request is considered to be an "emergency" and "time is of the essence", the relevant member of Security Supervisor will judge whether or not to provide the information without the submission of an appropriate form. Providing access to images to the Police or other law enforcement agencies without a completed standard form should be considered to be "exceptional" and not the University's standard practice, by either staff or law enforcement agencies. Other relevant agencies may not use standard forms to make requests for personal data.

However, any request should:

- Be clearly identifiable as from the agency in question i.e. in writing, on headed paper, and signed by an officer of the agency. The University should take any steps it deems

necessary to ensure as far as is practicable that the request is legitimate.

- Describe the nature of the information which is required.
- Describe the nature of the investigation (e.g. citing any relevant statutory authority to obtain the information).
- Certify that the information is necessary for the investigation.

Each request will be assessed on a "case-by-case" basis. The decision as to whether the University should provide CCTV footage will be taken by the Security Controller represented by the Secretary General or his/her deputy. If there is doubt as to whether information should be released the Information and Data Protection Commissioner should be consulted http://www.idp.al/index.php/en/.

Where Security Services Staff have contacted the police regarding images captured on the CCTV system for the purposes of security or the prevention or detection of crime then the police will not be required to provide a "Personal Data Request Form". Any disclosure made by the University to the police in these circumstances is considered to be in the legitimate interests of the University and in line with the purpose of the CCTV system.

Any unauthorized disclosure or misuse of CCTV data by staff is a serious matter and is considered a disciplinary issue.

7.2 Right of Subject Access

Where a potential data subject wishes to obtain access to/copies of the recorded CCTV images of him/her, he/she is advised to complete the form "Subject Access Request Form – CCTV Images" available via the Accessing your Personal Data section of the Data Protection web pages. The completed form should be returned to the ICTC Office with the other required documentation. The University's Data Protection web pages contain all relevant information regarding Subject Access Requests Form (SARs). The University has 30 calendar days to respond to a SAR.
The ICTC Office will process any SAR requesting CCTV footage in conjunction with Security Services. Where third parties can be identified from the footage, the images may have to be obscured to prevent such identification. If images of third parties cannot be suitably obscured, the University may not be able to grant the data subject access to the data.

8. COMPLIANCE

The University will at all times comply with the current Protection of Personal Data legislation. In doing so the University will also refer to any relevant guidance produced by the Office of the Commissioner on the Protection of Personal Data, in particular any specific codes of practice related to CCTV.
All staff dealing with CCTV equipment and recordings should be aware of the University Guideline on the Functioning of the CCTV system and the University's Notification on the Register of Data Controllers (http://www.idp.al/index.php/en). In addition these staff members should receive appropriate training to ensure they are aware of the correct operation of the system and handling of personal data.

Any misuse of information obtained from a video recording is a breach of the Data Protection Law. Any such breach is a serious issue and will result in disciplinary action being taken against the member of staff involved. In certain circumstances, individual members of staff may also incur criminal liability.

The Security Supervisor shall carry out a weekly check of paperwork to ensure all procedures are being complied with. Results of the audit shall be recorded in the Daily Register Sheet. The time noted on each of the DVR units shall be checked weekly by the Security Services Staff. This will be logged in a "System Time Check" sheet.

In line with best practice (and as outlined in the Guideline), the Security Supervisor will ensure that regular audits are conducted into the operation of the system.

9. REVIEW

A formal review of the University's CCTV Guideline and associated documentation will be carried out by the Security Supervisor on an annual basis. An evaluation of the system and equipment will also be undertaken annually by the Security Supervisor. All evaluations will be formally reported by the Security Supervisor to the Secretary General of Epoka University.

There are a number of forms associated with this policy. However, these are not included in the policy as these may, from time-to-time, be subject to minor changes in terms of content, format and layout. However, where the overall purpose of any form is changed or it is deemed that a form is no longer required, this would constitute a change of this Guideline and the Guideline must be reviewed and updated accordingly. The Security Supervisor is responsible for any amendments to the associated forms.

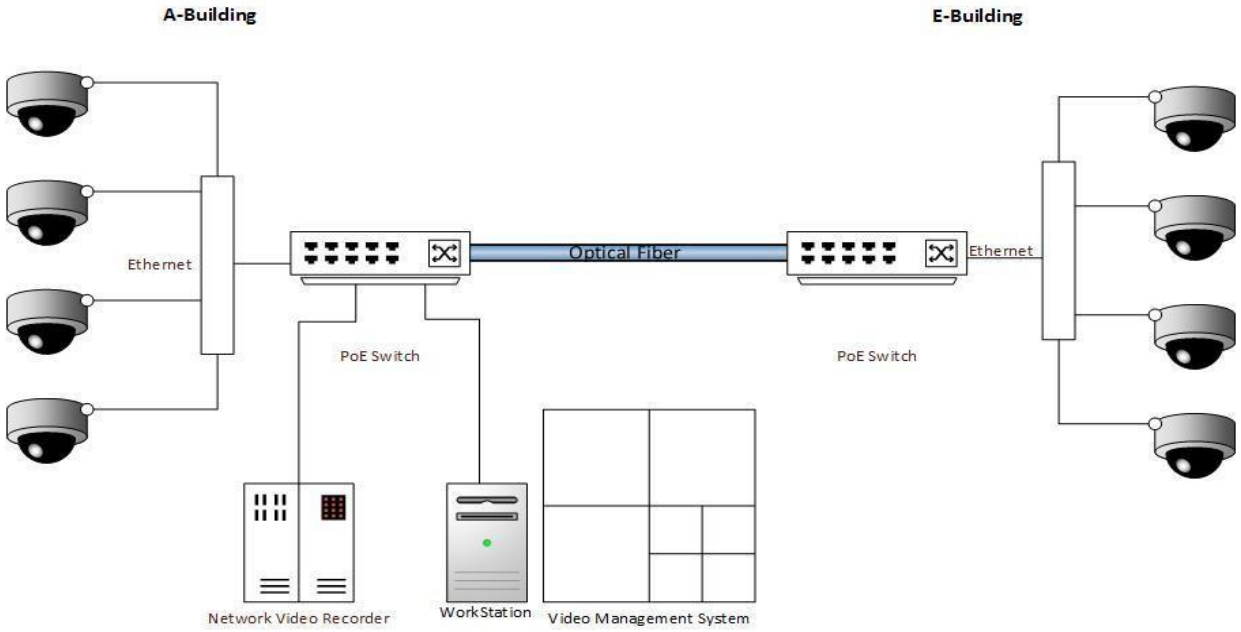
ANNEX I

Every video surveillance deployment is made up of cameras, video management software, servers and storage. The IP network is then the element that ties all these components into a converged network infrastructure.

All the IP Cameras are connected to the IP Network. The cameras are powered through the network from PoE switches. Network Video Recorder is installed on Server Room and all the cameras are managed and recorded to this NVR.

For live view of cameras or playback of recorded video, it is use Video Management System client installed on workstation and also through remotely connects to the NVR.

Logical diagram of the system is as follows:



Logical Diagram

IP Cameras

The following models are the IP Cameras installed in Epoka Campus. All cameras are Grand stream IP Cameras.

Grandstream GXV3611

For corridor and common places are installed Grand stream GXV3611. This is an indoor fixeddome IP Camera that can be easily mounted on walls or ceiling. This camera is for day surveillance.

Grand stream GXV3662 with standard kit

For Entrance there are installed Grand stream GXV3662. This is an IP66 camera, Vandal Resistant Fixed Dome, which can be installed in outdoor environments. It is a day and night vision surveillance camera.

This is an HD, 1.2 Megapixel IP Camera, it supports Motion Detection.

Grand stream GXV3662 with standard kit

For outdoor environments there are used also Grand stream GXV3662 with extra Wall Mount kit.

All cameras supports dual video stream and each stream can be configured differently in terms of compression format and level, frame rate and resolution. For example, one stream can be configured with maximum compression and low frame rate for storage purposes; another stream can be sent with higher frame rate and less compression and, therefore, less lag for live viewing.

Network Video Recorder

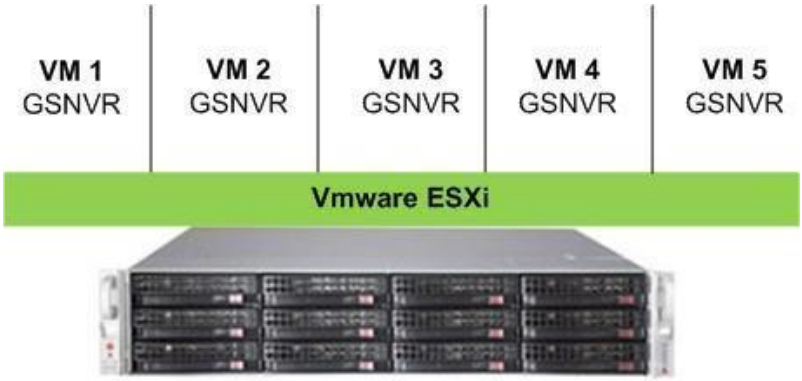
NVR is the system used for video recording. The system is based on SuperMicro hardware and Grand stream GSurf Pro NVR. This system is based on standard components found in the IT industry; this means you are not "locked" to proprietary NVR platforms with expensive licenses and support fees. With the proposed system, you can install software of your choice (except GSurf Pro, a number of other free VMS software packages are available like iSpy, AxxonSoft, ZoneMinder…etc). Specialized equipment is not needed since a storage solution treats video data like any other large group of files that can be stored, accessed and eventually deleted. Similar to the way a PC can "save" documents and other files, video can be stored on a server or PC hard disk.

The proposed NVR hardware for EPOKA campus are equipped with dual Xeon CPU, 32 GB of RAM and 18 TB of raw storage.

As a video recording application there are used Grandstream GSurf Pro NVR. This are free software package that provides the tools for monitoring and recording surveillance video streams for up to 72 IP Cameras. In order to cover all the cameras for both buildings, there are used virtualization. There are virtualized the hardware server with VMware ESXi 5.0 hypervisor and five virtual machines will be created. On each virtual machine there are installed Grandstream GSurf Pro NVR. One virtual machines is used to record video for A-Building, one virtual machines used to record video for Perimeter and Main Entrance area. Two virtual machines are used to record video for E-Building and one virtual machine are used to record video from Dormitory.

Even that there are three buildings, where are used one NVR installed on the campus Server Room.

The architecture of NVR will be as follows:

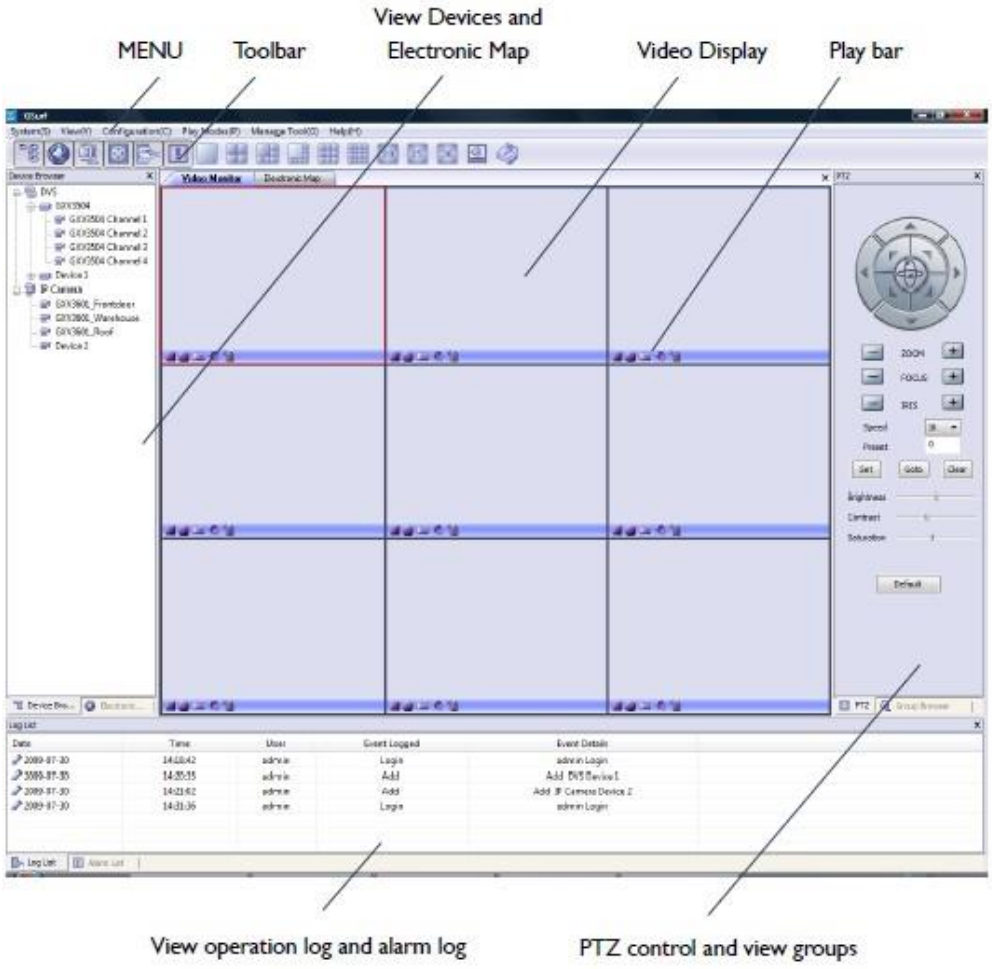


NVR Server

Technical specifications for Super Micro Server are as follows:

Processors:	2x Intel Xeon E5-2603 (1.8GHz/4-core/10MB/6.4GT-s QPI/80W) Processors
Memory:	32 GB (4x4GB) PC3L-10600R (DDR3-1333) Registered DIMMS Support for up to 512GB RAM
Storage Controller:	SATA Raid controller with support for RAID 0, 1, 5, 10
Hard Drive:	6x 3TB SATA 7200 RPM 3.5'' HDDs Support for up to 12x 3.5'' Hot Plug SAS2/SATA3 Hard Drives
PCI-Express Slots:	5x PCI-E 3.0 x8 slots (Lowprofile) Network Controller: 6x GbE NIC ports
Power Supply:	2x 920W Redundant power Supplies)
Management:	Dedicated IPMI 2.0 LAN management port
Form Factor:	2U rack mount
Warranty:	3 years

At the control Room (or to the room where all these cameras will be monitored) there are install a workstation where Grandstream GSurf Pro is installed.
This client PC will be used for live monitoring of cameras or playback recording. Grandstream GSurf Pro is a monitoring and recording system for up to 36 cameras. GSurf Pro supports remote viewing, control and recording from anywhere on the Internet or corporate network. The user interface was designed for ease-of-use to offer quick, easy access to cameras and recording in the system.

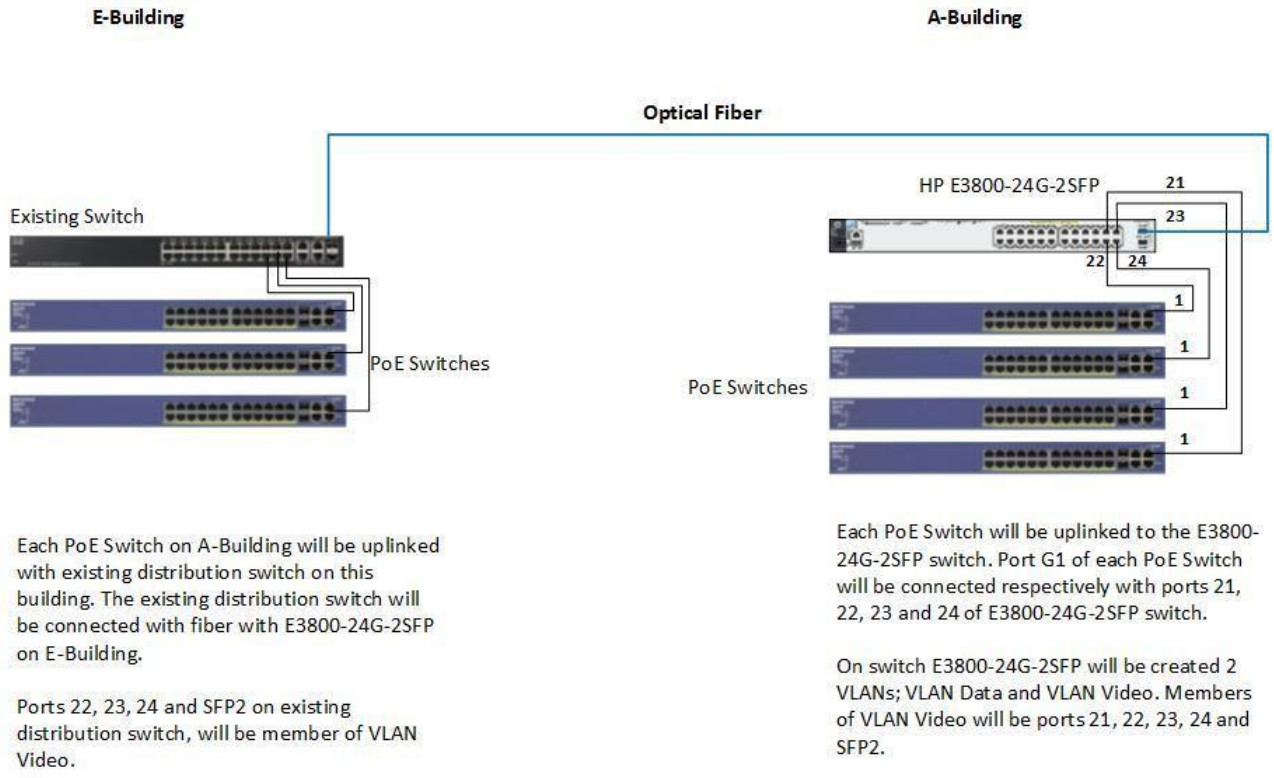


IP Network

IP Cameras surveillance system of Epoka University relies on an IP network infrastructure to link all components.
IP Network is composed by two components:

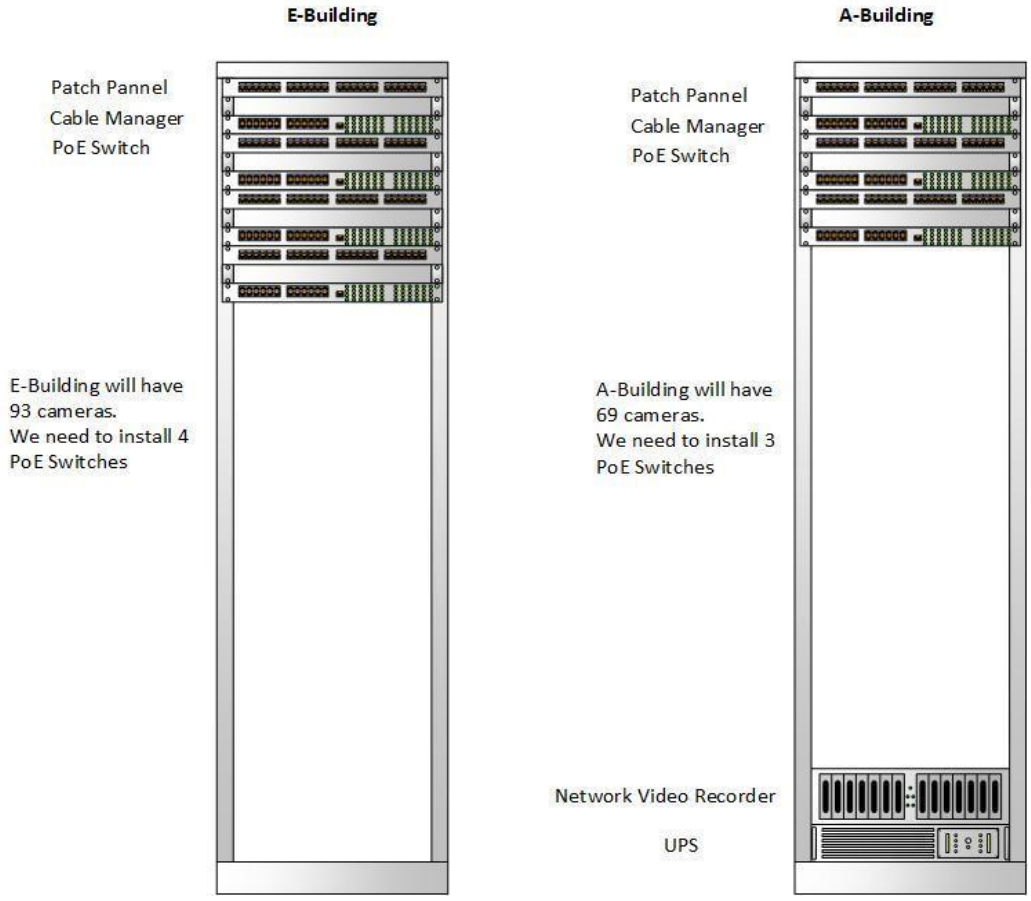
- PoE Network Switches
- Cabling

PoE Network Switches connect and power all the cameras. There are used Netgear Prosafe FS728TP switches. These are 24 ports 10/100 Mbps switches with PoE on all ports and 4 Gigabit RJ45 Uplink ports. 2 Uplink ports are dual personality which means, can be used as RJ45 for copper connection or SFP for fiber connectivity. Switches are manageable through an easy to use web interface. They support advanced features like VLANs, RADIUS Authentication, Access Lists, QoS, and Rate limiting….etc.



Switches Connectivity

For cabling there is used PANDUIT Cat.6, UTP cables.



Rack Organization