Pursuant to Article 9-b, paragraph 2, of the Law on Personal Data Protection ("Official Gazette of R. of Macedonia", no. 05/07, 103/08, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18), and provisions of the Rule on content and form of the act of performing video surveillance (Official Gazette of the Republic of Macedonia no. 158/10) and Article 27, paragraph 1, item 6 of the Statute of the South East European University, the University Board, at its meeting held on 09.09.2019 approved the following:

RULE ON VIDEO SURVEILLANCE PERFORMANCE AT SOUTH EAST EUROPEAN UNIVERSITY

I. Subject of regulation

Article 1

This Rule prescribes the content and form of the act of performing video surveillance at South East European University (hereafter: SEEU), which occurs as a controller, as well as technical and organizational measures that are implemented to ensure confidentiality and protection of personal data by performing video surveillance, the storage period of video surveillance, how to delete and how to make backup copies, and the rights and obligations of authorized persons who have access to the system for video surveillance.

II. Description of the video surveillance system

Article 2

(1) Video surveillance is done through cameras placed at SEEU where they are directed only to critical areas for SEEU.

(2) The recordings from the cameras are stored in DVR devices in the central server room at SEEU where the authorized person from the security service has access to these videos.

(3) The recordings taken from the video surveillance are stored in the hard drive of the DVR device in the central server room of SEEU.

III. The aim of performing video surveillance

Article 3

Video surveillance is done in order to ensure:

- protection of property, and
- providing control over entry and exit from the SEEU premises.

IV. Periodic assessment

Article 4

(1) Every two years SEEU (Security and Maintenance) evaluates the results of the system for performing video surveillance, especially for:

- the need for further use of the system for performing video surveillance;
- the aim or aims for performing video surveillance;
- possible technical solutions for the replacement of the system for performing video surveillance;
- statistical indicators of access to the recordings made from video surveillance, and
- the manner of utilizing the recordings.

(2) For the periodic assessment referred to in paragraph 1 of this Article, the Security Service prepares a report which is an integral part of the documentation for the establishment of the system of performing video surveillance.

V. Processing of personal data

Article 5

The following categories of personal data are processed through the system for video surveillance:

- the physical and physiological appearance of the parties entering and leaving the SEEU premises, and
- the physical and physiological appearance of SEEU.

VI. Technical measures

Article 6

SEEU provides the following technical measures for the protection and confidentiality of personal data processing through the performance of video surveillance as follows:

1. unique username for each authorized person;
2. password created by every authorized person, consisting of a combination of at least eight alphanumeric characters (of which at least one is a capital letter) and special characters;
3. username and password allows an authorized person to access the video surveillance system as a whole or individual applications;
4. automatic sign off from the video surveillance system after the expiration of a specified period of inactivity (no longer than 15 minutes), and re-activation of the system requires re-entry of username and password;
5. automatic rejection from the video surveillance system after three unsuccessful attempts to log in (entering the wrong username or password);
6. network software protective barrier (firewall) or router between video surveillance system and internet or any other form of external network as a protective measure against unauthorized or malicious attempts to enter or break into the system;

7. connecting the system for video surveillance into power grid through a device for uninterruptible power supply.

VII. Organizational measures

Article 7

(1) SEEU provides the following organizational measures for confidentiality and protection of personal data of processing by the video surveillance system:

1. limited access or identification of access into the video surveillance system so that only SEEU authorized persons have access to the video surveillance system;
2. each authorized person has limited access to the video surveillance system in terms of recording and downloading videos;
3. destruction of video recordings after the deadline for their storage, and
4. respect of technical instructions when installing and using the equipment for video surveillance.

(2) Upon request from the Facility and technical capacity Department, the Human Resources Office shall notify the IT Department for the engagement of any authorized person with a right of access to the system for video surveillance, to be given a username and password, and after termination of the employment or engagement the username and password will be deleted or locked for further access.

(3) The locks and deletions referred to in paragraph 2 of this Article shall be made at any other change in the employment status or the status of engagement of any authorized person who has an impact on the level of access allowed to the information system.

VIII. Recording access and inspection

Article 8

For access and inspection to personal data processed by the system for video surveillance, SEEU maintains records that contain the following data:

- name and surname of the authorized person;
- date and time of access;
- aim of access;
- date and time of the recording which is accessed;
- date and time, name and address of the user who is given a recording from video surveillance;
- type of media on which the recording of the video surveillance is kept.

IX. Authorized persons for processing personal data through video surveillance

Article 9

(1) Access to, and inspection of, personal data processed by the system for video surveillance is available only to authorized persons for the control of critical areas.

(2) The authorized persons referred in paragraph 1 of this Article will, prior to the commencement of work or before accessing the system for video surveillance, sign a statement of confidentiality and protection of personal data.

(3) The form of the statement referred to in paragraph 2 of this Article shall be a part of this Rule (Form No. 1).

X. Terms for storage of recordings from video surveillance

Article 10

(1) Recordings from the video surveillance system are stored on the hard drive of the PC where access is restricted to the Information System administrator and other authorized persons that control the critical areas for SEEU.

(2) Recordings from the video surveillance are kept 15 days; after the deadline they are automatically deleted from the hard disk where they are stored.

(3) Recordings taken from the video surveillance system can be stored for a longer period of time than the period specified in paragraph 2 of this Article, if required by law, but not longer then the fulfilment of specific objectives.

XI. Announcement for the conducting of video surveillance

Article 11

(1) In critical areas in SEEU there is notification posted (in clear and visible locations) that video surveillance is being conducted, which contains the following information:

- announcement that video surveillance is being conducted;
- the name of the controller who conducts the video surveillance; and
- the way to obtain information on where, and for how long, recordings from the video surveillance system are kept.

(2) The form for the announcement, as referred to in paragraph 1 of this Article, shall be a part of this Rule (Form no. 2).

XII. Technical specifications of the equipment

Article 12

(1) For conducting video surveillance a system is used that consists of static cameras that observe internal and external spaces, digital and analogue, maximum recording resolution of 2M pixels; these do 24-hour recording without the ability to zoom, and contain support to record in dark areas.

(2) The video surveillance system can be accessed from two workstations—these are two personal computers in the Security Service.

XIII. Plan where the system of video surveillance is set

Article 13

The graphic layout of the video surveillance system, the space where video surveillance is carried out, the angle of coverage of the area covered by video surveillance, as well as the map with the location of where the cameras are positioned, are contained in the plan which is an integral part of this Rule (Annex No. 1).

XIV. Subsidiary application

Article 14

During processing of personal data through the video surveillance system, other provisions of the Rule on Technical and Organizational Measures for Securing Confidentiality and Protection of Processing Personal Data (Official Gazette of the Republic Macedonia No. 38/09 and 158/10) are applied.

XV. Final provision

Article 15

This Rule enters into force on 01.10.2019.

Form 1

Based on the provisions of the Law on Protection of Personal Data ("Official Gazette of the Republic of Macedonia" No. 7/05, 103/08, 124/10 and 135/11, 43/14, 153/15, 99/16 and 64/2018), on the date ....., .20..... , I the undersigned, make the following

STATEMENT

for confidentiality and protection of personal data processing through the video surveillance

I the undersigned, ...,

(Name and Surname)

..... in accordance

(Title of work) (Department)

with the Rule for processing video surveillance at SEEU for the protection of personal data, accept and acknowledge the obligation that:

- I will respect the principles of protection of personal data through video surveillance;
- I will apply technical and organizational measures to ensure confidentiality and protection of personal data and will keep confidential personal data, and measures for their protection;
- Will apply technical and organizational measures for access and insight to personal data processed by the system for video surveillance, which prevents unauthorized and unregistered access and insights to the records from video surveillance system;
- Will process personal data in accordance with the guidelines provided by the controller;
- To the third parties, out of the controller and to the others from the controller, I will not issue any personal data from video surveillance records or any other personal information that is available to me and that I might learn or will learn in performing video surveillance in the controller, unless this will be required by law.

Signature,

.....

Form 2

ANNOUNCEMENT FOR CONDUCTING VIDEO SURVEILLANCE

Annex no.1

Plan where the system of video surveillance is set

1. Video surveillance is done through cameras installed at critical areas in SEEU where they are targeted only for control of the critical areas for SEEU.
2. Graphical representation of the placement of the camera for video surveillance: