APPROVED AT TUM SENATE MEETING OF 24.11.2015, MINUTES NO 3

REGULATION ON SUPERVISION BY VIDEO MEANS WITHIN THE PUBLIC INSTITUTION "TECHNICAL UNIVERSITY OF MOLDOVA"

I.GENERAL PROVISIONS

1. In the current context, the security of objectives cannot be ensured without effective video surveillance, allowing both real-time monitoring of suspicious events and persons and the recording of video images.

2. These video surveillance systems are mainly aimed at retail and commercial premises as well as public access offices.

3. At the same time, the use of such a system includes certain responsibilities and guarantees on the part of the system owner regarding the processing and protection of personal data recorded in the system, duties and regulations described in the Law no. 133 of 18.07.2011 on the protection of personal data.

4. For this reason it is necessary to establish a security regulation on video-surveillance and the processing of personal data collected and recorded in the video-surveillance system.

II. THE PURPOSE OF THE REGULATION ON VIDEO-SURVEILLANCE IN WITHIN THE UNIVERSITY

5. The Regulation on video surveillance within the Technical University of Moldova (hereinafter the University) aims:

✓ Establishing a uniform set of rules governing the implementation and use of the video surveillance system, in order to ensure the security of persons and property, guard and protect property, real estate, valuables and materials with special regime, while respecting the obligations of the University, as data controller, according to Law no. 133 of 18.07.2011 and the security measures adopted for the protection of personal data, protection of privacy, legitimate interests and guarantee of fundamental rights of data subjects.

✓ Establishing the responsibilities for the administration and operation of the video-surveillance system, as well as for the drafting, endorsement and approval of documents related to these activities.

✓ The purpose of the use of the video system is to ensure the proper administration and functioning of the University, in particular for security control and guarding. The video system is also necessary to support the security policies laid down by the regulations

governing the protection of personal data and contributes to the fulfillment of the tasks of the security structure.

✓ This Regulation describes the measures that need to be taken by the University to protect the personal data that are processed through the video surveillance method, privacy and other fundamental rights and legitimate interests of the subjects.

III. AREAS UNDER SURVEILLANCE

6. Video surveillance cameras shall be located in visible places. Any covert use is strictly prohibited, except where expressly provided for by law.
7. The video surveillance cameras shall be placed according to Attachment no.1 to this Regulation.
8. Areas where people can reasonably count on privacy, such as service desks and toilets, are not monitored.

IV. PERSONAL DATA COLLECTED THROUGH THE VIDEO- SURVEILLANCE SYSTEM

9. The video surveillance system is equipped with a motion detector. All cameras operate 24/24 hours and are regularily fixed.
10. When the video surveillance system is put into operation, the authorized person shall be instructed on the settings of the video monitoring system, the confidentiality regime and the right of access to the information processed in the system.

V.PURPOSE LIMITATION

11. The video-surveillance system will be used only for the purpose for which it is notified, with no particular aim to obtain information for internal investigations or disciplinary proceedings, except in situations where a security incident occurs or criminal behavior i s observed (in exceptional circumstances the images may be passed on to the competent bodies in disciplinary or criminal investigations).
12. In order to protect the privacy of subjects other than those directly targeted, the video system shall be equipped with mechanisms that provide for image blurring (if necessary) to anonymize the whole image or part of it, as appropriate.
13. The responsible person will manage access to the video surveillance system only with the written consent of the University management.

VI. SPECIAL CATEGORIES OF PERSONAL DATA

14. The purpose of the University's video monitoring system is not to capture (e.g. by selective focusing or targeting) or process images (e.g. indexing, profiling) which constitute special categories of personal data.

VII. ACCESS TO AND DISCLOSURE OF PERSONAL DATA

15. Access to real-time video footage is restricted to a limited number of University employees, who can be individually identified according to a list approved by the University management.
16. Access to the video images and/or the archive where the recorded images are stored is permitted only to the person responsible in accordance with the University Security Policy and only with the written consent of the management.
17. Viewing and/or making copies from the temporary files in which the video images are stored is permitted only with the written consent of management.
18. When copies of the temporary files in which the video images are stored are requested by the law enforcement bodies of the Republic of Moldova, exercising their powers according to the law, access is granted only with the written consent of the University management.

VIII. PROTECTION OF PERSONAL DATA INFORMATION SYSTEM IN WHICH VIDEO IMAGES ARE STORED (PROCESSED)

19. In order to secure the personal data information system in which the video images are stored (processed), the following technical and organizational measures shall be applied:
▪ the personal data information system in which the video images are stored (processed) is kept in a specially equipped room;
▪ The University's Data Protection Officer and Security Officers will be consulted prior to the purchase or installation of any new surveillance system;
▪ all systems must comply with the security requirements described in the legislation (GD no. 1123 on the approval of the requirements for ensuring the security of personal data);
▪ physical access to the personal data information system in which they are stored (processed) video images has only the designated responsible person and the University management;
▪ access to the processed video is restricted by entering a string of passwords;
▪ in the event of power disconnection, the personal data information system in which the video images are stored (processed) is equipped with an autonomous power supply (UPS);
▪ the personal data information system in which the video images are stored (processed) is equipped with a firewall providing network protection;
▪ the equipment is installed in such a way that only those areas identified in the risk analysis as requiring additional protection are under surveillance;
▪ Video surveillance system users are instructed not to monitor such areas;
▪ The University constantly updates the list of persons who have access to the personal data information system in which the video images are stored (processed), which describes in detail their access rights.

IX. ACCESS CONTROL

20. The images captured by the video surveillance system are viewed in real time on the monitors in the access control room, which is a secure room and the monitors cannot be seen from the outside.
21. The access control room is located in the University's main building.
22. Unauthorized access to the Control Room is prohibited. Access is strictly limited to authorized employees: personnel with physical security and access control functions, the System Administrator, Information Security Officers, and University management.
23. On a case-by-case basis, access to the Control Room may be granted to persons other than those mentioned above, only upon authorization from the University Security Officer. These persons will not have access to the personal data processed in the video-surveillance activity, their access being allowed strictly for the performance of the work mentioned in the authorization from the University Security Officer, (processed) video images has only the designated responsible person and the University management;
▪ access to the processed video is restricted by entering a string of passwords;
▪ in the event of power disconnection, the personal data information system in which the video images are stored (processed) is equipped with an autonomous power supply (UPS);
▪ the personal data information system in which the video images are stored (processed) is equipped with a firewall providing network protection;
▪ the equipment is installed in such a way that only those areas identified in the risk analysis as requiring additional protection are under surveillance;
▪ Video surveillance system users are instructed not to monitor such areas;
▪ The University constantly updates the list of persons who have access to the personal data information system in which the video images are stored (processed), which describes in detail their access rights.

IX. ACCESS CONTROL

20. The images captured by the video surveillance system are viewed in real time on the monitors in the access control room, which is a secure room and the monitors cannot be seen from the outside.
21. The access control room is located in the University's main building.
22. Unauthorized access to the Control Room is prohibited. Access is strictly limited to authorized employees: personnel with physical security and access control functions, the System Administrator, Information Security Officers, and University management.
23. On a case-by-case basis, access to the Control Room may be granted to persons other than those mentioned above, only upon authorization from the University Security Officer. These persons will not have access to the personal data processed in the video-surveillance activity, their access being allowed strictly for the performance of the work mentioned in the authorization from the University Security Officer.

X. TECHNICAL AND ORGANIZATIONAL MEASURES TO PROTECT THE VIDEO SYSTEM

24. The following technical and organizational measures have been introduced to protect the security of the video system and to enhance privacy protection:

✓ limiting the storage time of the footage, in compliance with security requirements and data retention legislation;
✓ the storage media (the servers on which the recorded images are stored) are in secure premises protected by physical security measures;
✓ all users with access rights to the video surveillance system have signed confidentiality agreements, by which they undertake to comply with the relevant legal provisions;
✓ users are granted the right of access only to those resources that are strictly necessary for the fulfillment of their service tasks;
✓ only the system administrators, appointed for this purpose by the controller, and the Security Officer have the right to access the files recorded in the system, at the request of the University management.

XI. ACCESS RIGHTS

25. Access to the stored images and/or the technical architecture of the video-surveillance system shall be limited to a limited number of persons and shall be determined by the duties specified in the job description, which shall indicate for what purpose and what type of access is granted.
26. The University imposes strict limits on who is eligible:
✓ to view the footage in real time: the images running in real time are accessible to the security officers and security guards assigned to carry out the surveillance;
✓ to view the footage: the viewing of the recorded images will be done in justified cases, such as cases expressly provided for by law and security incidents, by specially designated persons;
✓ to copy, download, delete or modify any material recorded by the video surveillance system.
27. All staff with access rights receive initial data protection training.
28. This procedure will be integrated into the training and guidance program for all users with access rights and responsibilities in the operation of the video surveillance system.
29. The Head of Sub-Division shall ensure that all subordinate staff involved in the operation of the video surveillance system are trained and briefed on all functional, operational and administrative aspects of this activity.
30. Immediately after the training each participant with access to the video surveillance system signs a confidentiality agreement.

XII. DISCLOSURE OF PERSONAL DATA

31. Any activity of disclosure of personal data to third parties will be documented and subject to a rigorous analysis of the necessity of the disclosure on the one hand, and on the other hand the compatibility between the purpose for which the disclosure is made and the purpose for which the data were originally collected for processing.
32. Any disclosure will be recorded by the System Administrator in a Disclosure Log.
33. The University is obliged to make available to the judicial authorities, upon their written

request, the video recordings in which the commission of acts of a misdemeanor/criminal nature is caught.
34. The video surveillance system is not used to verify program attendance or evaluate job performance.
35. In exceptional cases, but subject to the safeguards described above, access may be granted to other services within the University (Fire Protection, Human Resources) in the context of a disciplinary, accident or security investigation, provided that the information is to assist in the investigation of a crime, workplace accident or disciplinary misconduct that may prejudice the rights and freedoms of a natural or legal person.

XIII. HOW LONG VIDEO RECORDINGS ARE KEPT

36. Video recordings are kept for 30 calendar days, after which they are automatically deleted in the order in which they were recorded.
37. In the event of a security incident, the retention time of the video recordings may exceed the permissible program limits, depending on the time required to further investigate the security incident.

XIV. INFORMING THE PUBLIC ABOUT VIDEO SURVEILLANCE

38. Information to the public about video surveillance at the University is provided by pictograms.
39. The University guarantees to ensure that the rights of data subjects are respected in accordance with the laws of the Republic of Moldova. All persons involved in video surveillance activity and those responsible for the management of filmed images will comply with the University's procedures and regulations on access to personal data.

XV. INFORMING DATA SUBJECTS

40. The primary information of the data subjects shall be provided clearly and permanently, by means of an appropriate sign, with sufficient visibility and located in the area under surveillance, so as to signal the existence of the surveillance cameras, but also to communicate essential information on the processing of personal data.
41. Data subjects shall be made aware of the existence of the video-surveillance system and its owner by means of appropriate information notices, which shall include the purpose of the processing and identify the University as the controller of the data collected through video-surveillance.

XVI. EXERCISING RIGHTS OF ACCESS, INTERVENTION AND OPPOSITION

42. Throughout the storage period of personal data, data subjects have the right of access to personal data concerning them, held by the University, to request intervention (erasure/updating/rectification/anonymization) or to object to processing, in accordance with the law.
43. Any request to access, rectify, block and/or delete personal data as a result of the use of video cameras should be addressed directly to the University.

44. If the data subject has any further questions about the processing of personal data concerning him or her by the University, he or she may contact the management of the University.
45. The reply to the request for access, intervention or opposition shall be given within 15 calendar days. If this time limit cannot be met, the data subject shall be informed of the reason for the postponement of the reply and of the procedure to be followed for dealing with the request.
46. At the express request of the data subject, the right to view the recorded images concerning him or her may be granted or a copy may be sent to him or her. The images provided will be clear as far as possible, provided that the rights of third parties are not prejudiced (the data subject will only be able to see his/her own image, images of other persons who may appear in In the event of such a request, the data subject shall be obliged:

a. identify themselves beyond any suspicion (show their ID when attending the viewing), mention the date, time, location and circumstances of the surveillance cameras;
b. The data subject will also provide a recent photo so that the designated users can easily identify him or her in the footage.

47. The right of access may be refused where the exceptions provided by law apply. There may also be a need to restrict access where there is an obligation to protect the rights and freedoms of third persons, for example if other persons are included in the images and it is not possible to obtain their consent or if irrelevant personal data cannot be extracted by editing the images.

XVII. VIDEO MONITORING SYSTEM SECURITY AUDIT

48. The video monitoring system security audit maintains system logs of system or application
activity events and user activity.
49. In conjunction with the respective tools and procedures, video monitoring system security auditing allows to promote means to help achieve security objectives: tracking user actions, defining and establishing individual responsibility, reconstructing events, detecting intruders and event identification problems.
50. The video monitoring system security audit is intended to support:

✓ establishing the sequentiality of user or process actions;

✓ determine when, who or what stopped the system from functioning normally;

✓ solving the problem of intruder detection;

✓ detecting problems with the functioning of the computer system online.

XVIII. FINAL PROVISIONS

51. The Regulation on video surveillance within the IP "Technical University of Moldova" will be supplemented whenever there are changes in the legal provisions on the basis of which it was developed.
52. This Regulation shall enter into force on the date of its approval and adoption by the University Senate.

Annex 1
LIST OF LOCATIONS WHERE SURVEILLANCE CAMERAS ARE INSTALLED AT THE TECHNICAL UNIVERSITY OF MOLDOVA

I. Locations and public access areas in the study blocks:

1. 168 Ștefan cel Mare Boulevard - study block nr. 1, Accounting department hall: 2 cameras;
2. 9/7 Students Street - study block nr. 3, entrance hall (Orange): 9 cameras;
3. 9/7 Students Street - study block nr. 3, basement, Computer Centre Laboratory, 3-113 - 5 cameras;
4. 9/7 Students Street - study block nr. 3, 5th floor - laboratories: 501, 502, 503, hall: 4 cameras;
5. 39 Dacia Boulevard - study block nr. 9, 1st floor, entrance hall: 1 camera;
6. 39 Dacia Boulevard - study block nr. 9, 2nd floor, hall, dean's office: 1 camera;
7. 39 Dacia Boulevard - study block nr. 9, Roads, Materials and Construction Machinery Department, hall: 2 cameras;
8. 39 Dacia Boulevard - study block nr. 9, laboratories P-16; P-18; P-20; P-22: 4 cameras;
9. 9/19 Students Street, University Excellence and Design Technologies Acceleration Centre: 15 cameras.

II. Locations around buildings to protect outdoor spaces:
1. Outdoor University Park Riscani campus - 4 video cameras.