

REGULATIONS

**ON THE OPERATION OF THE VIDEO SURVEILLANCE SYSTEM
AT POZNAN UNIVERSITY OF TECHNOLOGY**



APPROVED

CHANCELLOR
of Poznan University of Technology
Łukasz Kalupa, Ph.D.

R E G U L A T I O N S

ON THE OPERATION OF THE VIDEO SURVEILLANCE SYSTEM

AT POZNAN UNIVERSITY OF TECHNOLOGY

HEAD
of the Security Office

Ryszard Grześkowiak, M.Sc., Eng.

COORDINATED BY:

Data Protection Officer:	
Information Security Officer:	
PUT IT System Administrator ASK "Z":	
PUT Legal Advisor:	

TABLE OF CONTENTS	page
§ 1. General provisions	- 7
§ 2. Purpose of surveillance	- 8
§ 3. Surveillance area and rules	- 9
§ 4. Procedure for the installation and integration of video surveillance devices	- 11
§ 5. Entitlement to data processing and access to recordings	- 12
§ 6. Personal data protection	- 12
§ 7. Securing and storing recordings	- 13
§ 8. Procedure for requesting to secure the recordings	- 13
§ 9. Final provisions	- 14
Attachments:	
No.1. REQUEST - form	- 17
No.2. REQUEST for securing/sharing video surveillance recordings	- 19
No.3. Information clause	- 21

§ 1. General provisions

1. These Regulations specify:
 - 1) the purpose and rules for the operation of the video surveillance system at Poznan University of Technology, hereinafter referred to as the "University";
 - 2) location of video surveillance devices;
 - 3) rules for the installation and integration of the video surveillance system with the University Video Surveillance Centre;
 - 4) rules for image recording and storage;
 - 5) rules for sharing video surveillance recordings.
2. The administrator of the video surveillance system is Poznan University of Technology.
3. Whenever the Regulations refer to:
 - 1) **Video surveillance** - it should be understood as an image recording system used by the University to ensure the safety of people and the protection of property;
 - 2) **CCTV system** – it should be understood as the technical infrastructure of the University's surveillance;
 - 3) **University Video Surveillance Centre** – a separate place on the premises of the University, equipped with surveillance systems and security infrastructure, in which designated employees of the Security Office and the Academic Guard carry out ongoing supervision over the situation on the premises of the University and coordinate the activities of the Academic Guard;
 - 4) **Recordings** - it should be understood as recording an image, GPS location data and descriptive data collected in the surveillance system;
 - 5) **Sharing a recording from the CCTV system** - it should be understood as providing a copy of a recording or enabling permanent acquisition of surveillance data by an entity authorized to do so by law, in particular the Police, the Prosecutor's Office, courts or other authorities conducting the proceedings;
 - 6) **Access to a recording** - it should be understood as enabling a person concerned by the data or a person who participated in the incident covered by surveillance to see the recording without providing a copy of the material and without the possibility of its independent recording or dissemination;
 - 7) **Technical Section** – it should be understood as designated employees of the Security Office of Poznan University of Technology, responsible for:
 - a) **maintaining the technical efficiency of the video surveillance system** (ensuring the continuous efficiency of cameras, recorders, servers, matrices used in the Security Office and other system components, ongoing clearance of faults and repairing breakdowns, periodic maintenance in accordance with the manufacturers' documentation and applicable procedures, control of the correct operation of devices and image quality);
 - b) **operation of the CCTV infrastructure** (managing devices and their configuration, maintaining, in cooperation with the Services and Operation Office, the transmission infrastructure used by the system, controlling the primary and secondary power supply of devices, monitoring the storage capacity and correct archiving of recordings, determining the location of cameras and justifying their installation, administering the surveillance system in terms of users and authorizations, making recordings available to authorized entities, conducting explanatory proceedings);

- c) development and modernization of the system** (preparation of the concept of system extension, participation in the development of technical documentation, estimation of investment costs, technical supervision over the implementation of new installations and acceptance of completed work);
- d) user support** (dealing with breakdown reports, providing support to organizational units in terms of the operation of the system, analysis of the needs for new camera points);
- e) documentation** (updating technical documentation, diagrams and configurations, keeping a register of breakdowns, repairs and inspections, preparation of information on the technical condition of the system);
- f) cooperation with contractors** (supervision over service companies, acceptance of maintenance and investment work, verification of the quality of service provided, reporting guarantee complaints);
- g) ensuring technical security** (making copies of system configuration, updating device software, eliminating technical vulnerabilities in cooperation with the Services and Operation Office and the Information Security Officer, ensuring compliance of the configuration with applicable security standards);
- h) budget planning** (preparing data for material and financial plans for the maintenance and development of CCTV, determining purchasing needs, planning the replacement of end-of-life devices).

§ 2. Purpose of surveillance

1. Video surveillance is carried out to:
 - 1) ensure the safety of students, employees and other persons remaining at the University;
 - 2) protect the University's property;
 - 3) counteract violations of public order and security on the premises of the University;
 - 4) document incidents related to threats to life, health, property, as well as other incidents whose obligation to register or control results from separate provisions, this applies, in particular, to conducting and documenting exams;
 - 5) support activities undertaken by the University Academic Guard;
 - 6) secure evidence for the purposes of proceedings conducted on the basis of legal provisions.
2. Video surveillance cannot be used to:
 - 1) constantly control the effectiveness of employees' work;
 - 2) interfere with the privacy of persons to the extent exceeding the purposes indicated in section 1;
 - 3) observe rooms in which the dignity or personal rights of persons remaining at the University could be violated, unless the applicable law provides otherwise.
3. These Regulations constitute a specification and development of the provisions contained in the Work Regulations of Poznan University of Technology in terms of the rules of using video surveillance at the University introduced on the basis of Article 22 ⁽²⁾ of the Act of 20 July 1974 Labour Code (Journal of Laws of 2025, item 277, as amended).
4. The legal bases for the introduction of the video surveillance system are the provisions of generally applicable law and internal legal acts, in particular:
 - 1) Article 50 section 1 of the Act of 20 July 2018 Law on Higher Education and Science (Journal of Laws of 2024, item 1571, as amended);
 - 2) Act of 22 August 1997 on the protection of persons and property;
 - 3) Regulation of the European Parliament and of the Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR).

§ 3. Surveillance area and rules

1. Surveillance rules

- 1) Surveillance must not violate the privacy of persons remaining on the premises of the University, and the rules of personal data protection must be strictly observed.
 - 2) **Cameras may be installed** in accordance with § 2 section 1 including, among others:
 - a) research and teaching laboratories – to protect expensive equipment, especially in places where high-value equipment is stored. Cameras may protect equipment from being stolen, damaged or accessed in an unauthorized way;
 - b) rooms with valuable equipment – e.g. computer rooms, server rooms, specialist laboratories, libraries (excluding areas that may expose user privacy);
 - c) equipment warehouses – all rooms in which equipment, laboratory materials, university devices are stored;
 - d) corridors, circulation areas, shared areas – places that are publicly available, surveillance may ensure the safety of people moving around the University (e.g. in the event of criminal incidents);
 - e) building entrances and exits – surveillance near entrances to buildings, including main doors, side doors, corridors, entrance halls;
 - f) parking spots and other external areas of the University – parking areas, driveways, pavements around buildings that can be observed to ensure the safety of vehicles and people moving around the University;
 - g) places where administrative and office work related to financial operations / transactions, storage of data subject to special protection is carried out (e.g. secretary's offices, Dean's offices, chancelleries, archives).
 - 3) Surveillance does not cover rooms made available to the university trade union organization, sanitary rooms, changing rooms, canteens and smoking rooms, unless the use of the surveillance system in these rooms is necessary to achieve the goal set out in § 2 section 1 and does not violate dignity and other personal rights.
 - 4) Video surveillance remains active 24/7.
2. Images from CCTV cameras are sent to the University Video Surveillance Centre, where the operators observe in real time the University's premises and facilities, receive and analyze the signals and make a decision to eliminate or minimize security-related threats.
 3. Cameras and devices not connected to the university-wide CCTV system may be used to conduct surveillance at the University after obtaining the Chancellor's written CONSENT issued on the basis of the submitted request specified in § 4 section 1 and expressed opinions.
 4. Cameras and devices included in the University's surveillance system and cameras and devices not connected to the university-wide CCTV system are maintained using organizational and technical resources ensuring an appropriate level of security, including in particular:

- 1) recordings which may be stored only in a location approved by the Services and Operation Office, at the same time it is not allowed to process surveillance recordings on unprotected external data carriers, external cloud services and other devices unprotected against unauthorized access without obtaining the consent of the Chancellor of Poznan University of Technology;
 - 2) limiting administrative access to devices and applications only to authorized persons;
 - 3) using individual user accounts protected by strong passwords and, if technically possible, multi-factor authentication;
 - 4) encryption of data transmission during network access to management devices and applications;
 - 5) registering access logs, configuration changes and login attempts;
 - 6) using network safeguards, in particular network segmentation and access restrictions using firewalls;
 - 7) maintaining up-to-date software of devices and management applications by regularly installing available security updates;
 - 8) device configuration, which covers, in particular, changing default access passwords and disabling by default active services and functions that are not used (e.g. remote access);
 - 9) correct configuration of time, time zone and synchronization of time to ensure the reliability and integrity of the recordings;
 - 10) using safe decommissioning procedures, including permanent deletion of data and restoring default settings - if justified.
5. The person(s) responsible for the processing and sharing of data and keeping the required documentation in the scope of the surveillance system operating outside CCTV, indicated in the request referred to in § 4 section 1, ensures the proper operation of the surveillance system, including cameras and recording devices, through their proper configuration, updating and periodic verification of the correctness of the configuration, operating parameters and the image recording process. In addition, they supervise the proper marking of the area covered by surveillance and verify whether the surveillance system is used only for the purpose and scope specified at the stage of its launch.
 6. A requester's superior indicated in the request referred to in § 4 section 1 is responsible for ensuring the organizational conditions for the operation of the surveillance system in accordance these Regulations.

§ 4. Procedure for the installation and integration of video surveillance devices

1. **Request¹** - a request form concerning video surveillance - assembly / installation / notification / inclusion of CCTV devices in the video surveillance system is submitted to the Chancellor of

¹ Request – a request form should be submitted according to the hierarchical order in the structure of the University

Poznan University of Technology through the Security Office (Attachment No. 1 to these Regulations).

2. Request - a request form should contain in particular:
 - 1) detailed justification (e.g. securing research equipment);
 - 2) indication of the location of the cameras;
 - 3) operating time of the devices (24 hours or at certain times);
 - 4) granted consents²;
 - 5) indication of persons authorized to view / register / share the surveillance data record;
 - 6) indication of the source of financing:
 - a) faculty or institute funds if the purchase is compliant with the financial plan of the faculty/institute;
 - b) university funds (e.g. the Chancellor's budget) in the case of larger investments or the need for financing from other funds (e.g. funds intended for security).
 - 7) a requester attaches the following to the Request:
 - a) a technical opinion specifying the parameters of devices, software, possibility of installing devices and estimated costs³,
 - b) an opinion expressed by the Data Protection Officer, taking into account:
 - the legal basis for data processing,
 - the assessment of the compliance of the purpose of processing (whether the purpose of installing the cameras is specific, clear and lawful, whether the surveillance system does not violate the principle of minimization – i.e. whether the cameras cover only the necessary areas, whether transparency and information obligation have been ensured, i.e. whether appropriate information for individuals concerned by the data will be provided in accordance with Article 13 of the GDPR, e.g. information plates).
3. The surveillance system operating at the University, in addition to the university-wide CCTV system, should be reported to the Security Office to determine the possibility of integration.
4. Stages of equipment installation:
 - 1) Equipment purchase

Purchases are made in accordance with the University's internal purchasing procedure. Legal regulations, including public procurement law, must be observed. The description of the subject of the contract is prepared by the Technical Section of the Security Office. The remaining procedures are performed by an applicant with the Public Procurement Office.
 - 2) Equipment assembly:
 - a) individual cameras are installed by the Technical Section of the Security Office;
 - b) for a larger number of devices, the assembly is commissioned to an external firm, selected in accordance with the University's internal purchasing procedure.

² as above

³ an opinion is issued by a designated employee of the Technical Section of the Security Office in consultation with a designated employee of the Services and Operation Office concerning the acceptance of the place of recording storage

- 3) Integration of devices with the technical infrastructure of the University's surveillance system⁴: after installing a camera, one should carry out its configuration, integration with the CCTV system, configuration in the surveillance management system, verification of the correctness of operation and updating technical and record-taking documentation. A device may be put into operation after positive completion of functional tests.

§ 5. Entitlement to data processing and access to recordings

1. Access to recordings

Only authorized persons have access to the surveillance records:

- 1) University Personal Data Administrator (Rector),
 - 2) University Data Protection Officer,
 - 3) Head of the Security Office,
 - 4) and other employees:
 - a) in the Security Office responsible for viewing, securing, sharing recordings and servicing CCTV equipment and systems,
 - b) in other organizational units of the University on the basis of a valid authorization issued by the Personal Data Administrator,
- after undergoing training in the protection of personal data.

2. Authorizations to process personal data contained in the video monitoring system:

- 1) are prepared by the Personal Data Administrator,
- 2) authorized persons sign an obligation to comply with the principles of personal data protection and security procedures.
- 3) each login to the system as well as operations performed on the recordings are subject to registration in system logs.

§ 6. Personal data protection

1. Data protection rules

The administrator of the video monitoring system fulfils the obligations arising from Article 13 of the GDPR and informs the persons covered by the surveillance system about the processing of their personal data (for this purpose, a layered information clause is posted). Detailed information on the processing of personal data can be found on the University's website.

2. Rights of persons covered by the surveillance system:

- 1) The right to access the recordings;
- 2) The right to demand the deletion of the data;
- 3) The right to submit a complaint to the President of the Personal Data Protection Office.

⁴§ 4 section 4 point 3 does not apply to devices operating outside the CCTV system

§ 7. Securing and storing recordings

1. Storage period

- 1) Recordings from the video surveillance system are stored for a period not longer than **14 days** from the date of their registration, in accordance with the principle of minimizing the retention period referred to in Article 5 section 1 letter e of the GDPR, unless:
 - a) they constitute evidence in the proceedings;
 - b) the Data Administrator has become aware that they could constitute evidence in the proceedings.
- 2) In the cases referred to in point 1 section 1) letters a and b, the storage period is extended until the lawful conclusion of the proceedings.
- 3) After the indicated period, the recordings are automatically overwritten or irretrievably deleted in a way that makes it impossible to recover them.
- 4) The established uniform period of storing the recordings is valid in all organizational units of the University. Deviations from this rule are unacceptable without the prior recommendation of the Data Protection Officer, consent issued by the Chancellor, or the Rector of PUT, unless separate provisions provide otherwise.

2. Protection against access by unauthorized persons

Recordings must be stored in a way that ensures their safety and prevents unauthorized access.

3. Storage extension

If a recording constitutes evidence in administrative or judicial proceedings, the storage period may be extended until the end of the proceedings.

§ 8. Procedure for requesting to secure the recordings

1. Request to secure a recording

- 1) If it is necessary to secure a recording, the natural person or the entity submitting a request to secure a recording must submit an appropriate request to the Security Office by providing the data specified in Attachment No. 2 to these Regulations.
- 2) The request is subject to registration and archiving.

2. Request procedure

The request should include the exact date, time and place of the recorded event. The request must be submitted within a maximum of 14 days from the incident.

3. Sharing recordings:

- 1) recordings may be made available only at the written request of authorized state bodies on the basis of legal provisions, at the request of authorized bodies;
- 2) in justified cases, e.g. to clarify events, the record may be made available for inspection by the person concerned, but always with other persons being anonymized;
- 3) the recording or data carrier made available is subject to encryption;

- 4) the operations of saving records are subject to listing the following: date, time, file name and the person performing the saving operation.

§ 9. Final provisions

1. Information obligation

- 1) The University provides information about the use of surveillance by:
 - a) graphic symbols;
 - b) the Rector's Ordinance, in which the Regulations are published;
 - c) an information clause regarding the processing of personal data, which specifies in particular:
 - the Data Administrator;
 - purposes and bases for data processing;
 - data storage period;
 - rights of persons concerned by the data;
 - contact details of the Data Protection Officer.

2. IT security

The recordings must be protected against unauthorized access, deletion, damage, theft and other cyber threats to ensure the confidentiality, integrity and availability of the information.

3. Conclusions and requests

- 1) In case of any doubts or need to report problems related to the installation and use of CCTV devices, please contact the Security Office by e-mail at kontrola.dostepu@put.poznan.pl
- 2) In accordance with the applicable law (in particular the Act of 10 May 2018 on the Protection of Personal Data and Regulation of the European Parliament and of the Council (EU) 2016/679 – GDPR), **video surveillance may be used only on the basis of relevant regulations and with the consent of the authorized bodies of the University**, in particular the Rector. Illegal or arbitrary placement of surveillance cameras may result in:
 - a) disciplinary liability,
 - b) official or criminal liability,
 - c) the need to immediately dismantle the CCTV system.

.....
place, date

Chancellor
of Poznan University of Technology
through
Security Office

.....
request No.

.....
place date of receipt

REQUEST - request form

1.	Name of the requesting unit			
2.	System name	Video surveillance - assembly / installation / notification / inclusion * of CCTV devices in the video surveillance system of Poznan University of Technology		
3.	Description of the notification - operating time of the devices	The description includes: purchase of an IP camera of the... type, scope of required work, including, e.g., purchase of assembly materials, making the cable route and installation of a camera, camera configuration, integration with the CCTV system, functional tests, as-built documentation. Operating time of devices: 24h/d or other in the case of surveillance operating outside CCTV.		
4.	Location	Facility:, room/s: Place of data recording:		
5.	Detailed JUSTIFICATION:	In the justification, take into account: what conditions generate the need to implement the project, including the impact on life and health safety, legal requirements, impact on operation continuity, risk of incidents and potential financial consequences and losses resulting from their occurrence.		
6.	Persons responsible for the processing and sharing of data and keeping the required documentation according to the obligations specified in § 3 sections 4 - 5 First name Surname - position – organizational unit – contact phone No. (applies only to the system operating outside the CCTV system)			
7.	Approximate costs (to be completed by the Requester together with a representative of the Technical Section)			
	item	quantity	unit price in PLN	gross value
item 1	Purchase of HIK-type IP camera (4–8 MP, PoE)	1	PLN 1,200. 00	1,200.00
item 2	Assembly materials (handles, box, connectors, electrical conduits, fastening elements)	1 set	PLN 400.00	400.00
item 3	5e/6 UTP cable with endings	1 set	PLN 400.00	400.00
item 4	Making the cable route and assembly of the camera	service	PLN 800.00	800.00
item 5	Camera configuration (IP addressing, software update, image parameters)	service	Technical Section	

item 6	Integration with the PUT video surveillance system (recorder/VMS, granting permissions, tests)	service	Technical Section	
item 7	Launching, functional tests and technical acceptance	service	Technical Section	
item 8	As-built documentation and update of the surveillance system documentation	service	PLN 200.00	200.00
item 9				
item 10				
			Total costs	3,000.00

8. Indication of the source of financing (cost centre, source of financing, allocation category, Project, Financial year)

9. Requester (title first name SURNAME - position - organizational unit – phone number)

signature

10. Requester's superior (title first name SURNAME - position - organizational unit – phone number)

I accept the request and send it for further processing

signature

OPINIONS

1. Technical Opinion (issued by the Technical Section and the Services and Operation Office. The opinion includes, among others: technical parameters of devices, installation possibilities, possibilities of inclusion in the University Video Surveillance System, estimated costs, determination of priority taking into account detailed justification, acceptance of the place of storing recordings, etc.)

Priority determination	priority I. - critical	priority II. - significant	priority III. - developmental

signature of the authorized person from the Technical Section

I accept the place of data recording

signature of the authorized person from the Services and Operation Office

2. Opinion of the Data Protection Officer (the opinion includes, among others: legal basis for data processing, assessment of the compliance of the purpose of processing, i.e. whether the purpose of installing cameras is specific, clear and lawful, whether surveillance does not violate the principle of minimization – i.e. whether cameras cover only the necessary areas, whether transparency and information obligation have been ensured - i.e. whether appropriate **information**, e.g. information plates, information clauses, **will be provided to individuals** concerned by the data, whether the obligation under Article 13 of the GDPR will be met).

signature of the Data Protection Officer

I accept the application. I agree to the following:

.....
.....

.....
Chancellor's signature

* underline as appropriate

.....
place, date

Security Office
of Poznan University of Technology

.....
request No.

.....
place date of receipt

REQUEST

for securing/sharing * video surveillance recordings

I. REQUESTER'S DETAILS

.....
First name and surname
.....
address
.....
phone No.
.....
Name of the institution requesting access to the recordings

II. DATE, TIME, EXACT LOCATION OF THE INCIDENT

.....
.....

III. SHORT DESCRIPTION OF THE INCIDENT

.....
.....
.....

IV. JUSTIFICATION OF THE REQUEST, INDICATION OF THE LEGAL BASIS

.....
.....
.....

.....
(Requester's legible signature)

☐ I agree ☐ I do not agree*

.....
legible signature of the person responsible for sharing the recordings

I acknowledge receipt of the recordings and declare that the received materials will be used only for the purpose indicated in the request.

.....
date, Requester's legible signature

* underline /delete as appropriate

INFORMATION CLAUSE

- concerning persons dealing with the request to share/secure recordings from the surveillance system

Pursuant to Article 13 sections 1 and 2 of the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Journal of Laws of the European Union L. 2016 No. 119, p. 1) – (hereinafter referred to as "GDPR"), we inform you that:

- 1) The administrator of your personal data is Poznan University of Technology, hereinafter referred to as the University, ul. Jacka Rychlewskiego 1, 61-131 Poznań, phone No. 61 665 3639, NIP: 777 – 00 – 03 - 699, REGON: 000001608,
- 2) In matters related to the protection of personal data, you can contact the Data Protection Officer by e-mail at iod@put.poznan.pl, or by phone on 61 665 3631.
- 3) Your personal data will be processed:
 - a) to deal with the submitted request – in connection with Article 18 GDPR,
 - b) to fulfill the legal obligations resting on the Administrator, in particular related to the archiving of documentation - in accordance with Article 6 section 1 letter c of the GDPR in connection with the Act of 14 July 1983 on the national archival holdings and archives (i.e. Journal of Laws of 2020, item 164).
- 4) The period of processing of personal data depends on the purpose for which the data is processed. The storage period will result from the provisions of law regarding archiving, records management and archival instructions on the basis of the Uniform File Classification List in force at the University.
- 5) You may request from the Administrator access to your data, their rectification, deletion, or limitation of processing.
- 6) You have the right to lodge a complaint to the President of the Personal Data Protection Office if you determine that the processing of personal data violates the provisions of the GDPR.
- 7) Providing personal data is a condition for dealing with the request. Refusal to provide personal data makes it impossible to deal with the request.
- 8) Based on the personal data provided, the Administrator will not make automated decisions concerning you, including decisions resulting from profiling.

UPDATE SHEET