Approved by Rector’s directive No 164 of 22 October 2018

Date of entry into force: 22 October 2018

Rules for the Use of Security Equipment and Data Processing

1. General provisions

1.1 The Rules for the Use of Security Equipment and Data Processing regulate the use of security equipment and data processing at Tallinn University of Technology (hereinafter referred to as "the university").

1.2 The university uses security equipment in compliance with the requirements set out in the General Data Protection Regulation of the European Union, the Personal Data Protection Act and the Security Act of Estonia and the advisory guidelines on processing and protection of personal data provided by the Data Protection Inspectorate for the implementation of the legislation.

1.3 The security equipment is used to protect the property in the university buildings and territories and to ensure the access and security of persons.

1.4 Security equipment is used:
1.4.1 to allow the passage of persons and property;
1.4.2 to prevent a situation posing a threat to the preservation of the property or security of persons;
1.4.3 to respond to an emergency situation;
1.4.4 in the event of damage to property or a person, to identify the person who caused the damage or committed the offence.

2. Definitions used in the Rules

2.1 For the purposes of these Rules, security equipment is alarm or surveillance equipment which is intended to detect an intrusion, any other attack or any potential threat to a guarded object.

2.2 For the purposes of these Rules, alarm equipment is a set of equipment which is intended to detect any potential threat to a person or property or any attack made against a person or property and to transmit an alert.

2.3 For the purposes of these Rules, surveillance equipment is a set of equipment which transmits or records a picture or an electronic signal and which is intended:
2.3.1 to keep guard of a territory, person, item or process;
2.3.2 to determine the location of a territory, person or item or the place at which a process is occurring;
2.3.3 to detect any potential threat to a person or property;
2.3.4 to detect any attack made against a person or property and to transmit an alert.

2.4 For the purposes of these Rules, surveillance equipment is divided into:
2.4.1 the access control and security system;
2.4.2 the video surveillance system.

3. Use of the access control and security system and data processing

3.1 The access control and security system is used and its data are processed only for the purposes of ensuring access of persons and protection of property.

3.2 The Security Division of the university may issue non-personalised data of the access control and security system on the basis of a reasoned written request of the head of the structural unit.

3.3 Personalised data of the access control and security system may be issued to the person himself/herself and to the committee set up for proceedings or body representing the state in proceedings.

3.4 The data of the access control and security system shall be preserved for up to 1 year.

4. Installation and use of the video surveillance system and data processing

4.1 The video surveillance system is used and its data are processed for the purposes of ensuring the security of persons and property.

4.2 When installing and using a video surveillance system, the installer and user shall ensure that no excessive damage is caused to the legitimate interests of the data subject by the video surveillance system.

4.3 If necessary, a data protection impact assessment shall be conducted by the installer and user before the video surveillance system is installed. The decision on the need for a data protection impact assessment shall be taken by the coordinator for protection of personal data and state secrets.

4.4 In the case of an installed video surveillance system, an analysis of the risks and the measures taken to mitigate them shall be performed by the user, if necessary.

4.5 People shall be notified of the use of a video surveillance system in the university buildings and territories by placing stickers with the image of the video camera and the contact details of the Security Division in a visible position in front of the area under surveillance.

4.6 The video surveillance system must be configured so that each authorised user has his/her own username and password to access the system.

4.7 The video surveillance system shall enable to trace back who and when processed (viewed, changed, deleted, saved) the data and which data where processed.

4.8 The data of the video surveillance system may be processed by the staff of the university's Security Division (hereinafter referred to as "the Security Division") and the company providing security services to the university (hereinafter referred to as "the security guards") in accordance with the authorisations granted and code of practice.

4.9 The security guards monitor the video camera images in real time in accordance with the code of practice, in the event of suspicion of a threat, in the event of an emergency or on receipt of notification of an offence and review video surveillance system recordings where this is justified.

4.10 When using the video surveillance system, the employees of the Security Division and the security guards shall make sure that the data cannot be accessed by unauthorised persons.

5. Granting access to video surveillance system data

5.1 In the event of a security incident, a person can turn to a public authority, to whom the relevant video recording will be issued.

5.2 In the case of suspicion of a security incident, the person can check the recording of the incident by submitting a written request for reviewing the video recording to the Head of the Security Division, stating the reason for reviewing the recording and the time and place where the incident took place.

5.3 The Head of the Security Division shall provide feedback to the person and give recommendations for future action.

5.4 The public authorities and their employees who handle incidents and who are legally entitled to request access to the university's video surveillance system recordings shall submit a request for access to the data in a form that can be reproduced in writing.

5.5 The request shall indicate the operation in connection with which access to the recording is requested and the basis and purpose of access to the data laid down by law.

5.6 If a recording is used in the resolution of a security incident, criminal or misdemeanour proceedings, the recording may be preserved until the end of the relevant proceedings.

5.7 A video surveillance system recording is preserved for 2 to 6 weeks from the date of recording. As an exception, video surveillance system recordings containing security incidents are preserved depending on the deadlines of handling the specific cases.