Approved by Rector's directive No 28 of 6 August 2024

In force from: 06.08.2024

Security Management Regulations

1. General provisions

1.1 The Security Management Regulations (hereinafter referred to as "the Regulations" apply to all persons staying on the properties of Tallinn University of Technology (hereinafter referred to as "the university") and in the buildings located there.
1.2 The Regulations govern the implementation of the measures required to protect the property owned or used by the university and to ensure the safety of individuals on the premises.
1.3 The Regulations do not apply to the university's:
1.3.1 fire safety management;
1.3.2 information security policy;
1.3.3 cyber security measures;
1.3.4 protection of personal data;
1.3.5 protection of state secrets and classified information of foreign states.
1.4 Security at the university is managed by the Security Division of the Real Estate Office, whose primary responsibility is to implement the necessary measures to protect the property owned or used by the university. These measures include:
1.4.1 resolution of security incidents, incl. participation in crisis management;
1.4.2 drawing up, disseminating and providing training on security procedures and guidelines;
1.4.3 carrying out security risk analyses;
1.4.4 ordering security services;
1.4.5 exercising supervision over and developing the security services;
1.4.6 managing and developing the security systems;
1.4.7 planning and organising the maintenance of the security systems;
1.4.8 managing access rights;
1.4.9 organizing property and liability insurance and , incl. settling insurance claims.
1.5 In a structural unit, the designated representative for security is either the head of the unit or a person appointed by the head (hereinafter referred to as the "representative of the structural unit "), who:
1.5.1 coordinates the security of the structural unit, in cooperation with the employees of the Security Division;
1.5.2 assesses the structural unit's protective measures and recommends adjustments to the Security Division;
1.5.3 approves requests for access to the premises of the structural unit.

2. Protective measures

2.1 In order to protect individuals on the premises of the university or the property owned or used by the university, the following measures are implemented to mitigate risks:
2.1.1 ordering security services;
2.1.2 implementation of security systems;
2.1.3 property and liability insurance.
2.2 Organization of security services
2.2.1 Security services are provided by a contracted security company under a framework agreement, which includes manned guarding, technical surveillance, and patrolling services.
2.2.2 The security company's responsibility is to provide services on the university premises with an aim to ensure the safety of individuals in the university and the security and protection of university property.
2.2.3 The security systems installed on university properties and in university buildings are monitored and managed centrally from the university's security control centre.
2.2.4 Upon organizing the security and protection of university properties, the security company shall follow the framework agreement, applicable legislation governing security services, the university's legislation, the guidelines, and instructions approved by the Security Division.

2.2.5 To arrange event security or request additional security services, a request must be submitted through the self-service portal at least 5 working days prior to the event. Additional costs shall be covered by the event organizer as outlined in the effective security services agreement.
2.3 Implementation of security systems
2.3.1 Maintenance and development of security systems is provided by qualified security companies under framework agreements.
2.3.2 The university uses a combination of access control and security systems, which are managed using an access control device. If necessary, the university also uses identification codes or biometric identification and authentication devices, along with monitoring video surveillance cameras installed across the campus and within the buildings.
2.3.3 The descriptions and security grades are presented in Annex 1 to the Regulations.
2.3.4 The Security Division, in collaboration with the representative of the structural unit, maps the rooms used by the unit, identifying the risks and protective measures associated with each room and determining the appropriate security grades.
2.3.5 If the representative of a structural unit finds that the current security measures are inadequate, the potential impact and likelihood of the risk are assessed. If necessary, enhanced security measures are then implemented.
2.4 University's property and liability insurance
2.4.1 Buildings and registered properties are insured against fire, water damage, natural disasters, burglary, theft, vandalism, and damage to electronic equipment.
2.4.2 Liability arising from activities, as well as from the ownership and management of buildings, premises, and property, is covered by civil liability insurance.
2.4.3 Liability for occupational accidents involving university employees is covered by the employer's liability insurance.
2.4.4 The university's Chief Financial Officer sets the excess limits of insurance contracts, and the structural unit that incurred the damage is required to cover a share of the excess.

3. Access rights management

3.1 The university's premises (restricted areas/buildings/rooms) can be accessed by using access devices, such as touch-free access control cards, chips, or registration numbers of vehicles associated with a person.
3.1.1 Access rights are granted to persons who have a university user account, i.e. UNI-ID.
3.1.2 All access devices are personalised, with no user- or university-related data printed on them, except for ISIC cards issued to students.
3.1.3 A person can have only one active access device.
3.1.4 An employee's access device is assigned the access rights associated with the person's workplace, incl. access to indoor parking lots at the person's workplace, rights associated with his/her position, and access to public spaces used by the employee's structural unit.
3.1.5 In indoor parking lots equipped with number recognition systems, the employee's vehicle is linked to his/her access device if the employee has provided his/her vehicle's registration number.
3.1.6 Students' ISIC cards are assigned access to their study rooms from 7 AM to 10 PM by default, and 24/7 access to the library.
3.1.7 Persons from outside the university who have a university user account (UNI-ID) are granted access rights to fulfil their contractual obligations.
3.2 Ordering access cards
3.2.1 To order access cards, the representative of the structural unit or the person responsible for the procurement contract submits a request to the Real Estate Office through the self-service portal.
3.2.2 Students order ISIC cards through the Federation of Estonian Student Unions. ISIC cards that include the functions of a bankcard are issued by the banks.
3.2.3 The structural unit covers the costs associated with issuing access devices.
3.3 Requesting, assigning and altering access rights
3.3.1 To obtain or alter access rights, a request to add a facility to the access device must be submitted through the self-service portal on the intranet.
3.3.2 An employee has the right to request access rights for himself/herself, a student or an external contracting party, with approval from the employee's direct superior.
3.3.3 Access to the premises of other structural units can be requested only with the approval of the representative of the other structural unit.

3.3.4 A student has the right to request access to the premises of student organisations, with approval of the Chairman of the Student Union.
3.3.5 External contracting partners have the right to request access to fulfil their contractual obligations, provided the request is approved by the representative of the structural unit or the person responsible for the procurement contract.
3.3.6 Contracted service providers responsible for maintenance, including system maintenance, are not granted independent access rights to premises with security grades 3 and 4. Service providers may conduct maintenance of the premises and system maintenance only in the presence of either the premises user or a responsible specialist from the Real Estate Office.
3.4 Rights and obligations of an access card user
The user:

- shall handle the access device prudently - protect the card against forgery, alteration, exposure to high temperature, mechanical damage and strong electric fields;
- shall use the access device only for work or professional purposes or any other purpose for which the access device was issued;
- when exiting a room equipped with an access control card reader, shall ensure that the door is closed and the alarm system of the room is activated if he/she is the last person to leave;
- in case of loss of or damage to an access card, inform, as soon as possible, the Security Division by calling 620 2112, who shall organise deactivation of the access card;
- in case of loss of or damage to an access card, pay the costs of issuing of a new card;
- compensate the university for damage caused by violation of the obligations of an access card user.

It is prohibited for an access card user:

- to authorise third persons to use the access card;
- to open doors or rooms for persons who are not authorised to enter the rooms;
- to leave the doors supplied with access control readers unlocked.
- to leave the room without activating the alarm if he/she is the last person to leave;

3.5 Revoking access rights
3.5.1 An access device is deactivated immediately upon deactivation of the university user account (UNI-ID).
3.5.2 The access devices of external contracting partners are deactivated immediately after the termination of the contract.
3.5.3 In an employee of an external contracting partner ceases to participate in the execution of the contract, the representative of the structural unit or the person responsible for the procurement contract must notify the Real Estate Office via the self-service portal on the intranet and the access device must be deactivated immediately.
3.5.4 ISIC cards are automatically deactivated either upon expiration or when students are exmatriculated.

4. Room maintenance and localization in emergencies

4.1 Employees of the Real Estate Office and employees of external contracted service providers are granted access rights in order to:
4.1.1 carry out routine cleaning, maintenance and contract work;
4.1.2 enable prompt intervention in emergency situations.
4.2 Employees of the Real Estate Office and employees of external contracted service providers may enter the premises of another structural unit to perform their duties, provided the room's user has submitted a service request through the self-service portal.
4.3 If an accident occurs on the premises, employees of the Real Estate Office and contracting partners are authorised to enter the premises and eliminate the threat.
4.4 Requests for cleaning and maintenance of utility systems shall be submitted and accidents shall be reported in accordance with the procedure established by the Real Estate Office.

5. Using data from security systems

5.1 The processing of data from security systems is governed by the order "Rules for the Use of Security Equipment and Data Processing".
5.2 The room usage log, excluding personal data, is forwarded to the data warehouse for generating various usage reports.

6. Monitoring

6.1 The employees of the security company monitor the university premises around the clock and ensure that the alarm system of the facilities is activated outside the opening hours of the buildings.
6.2 The Security Division, in cooperation with the structural units, conducts annually an inspection of access rights.
6.3 A structural unit shall keep records of the access devices of its contracting partners and inform the Security Division of any changes regarding the users of the access devices.