Regulations for ensuring security in buildings of the University of Tartu

Based on clause 15 (2) 16) and (3) of the Statutes of the University of Tartu, adopted by the Senate of the University of Tartu Regulation no. 11 of 21 July 2014 and approved by the Council of the University of Tartu Resolution no. 18 of 29 July 2014, I establish the regulations for ensuring security in the buildings of the University of Tartu. [effective as of 7 January 2016]

I. General provisions

1. The regulations for ensuring security in the buildings of the University of Tartu (‘university’) (‘regulations’)
   1.1. determine the conditions, measures of and requirements for ensuring security in the buildings (‘building’ or ‘buildings’) and rooms (‘room’ or ‘rooms’) that are owned or used by the university;
   1.2. establish the conditions for planning and implementation of university security systems;
   1.3. govern the organisational matters of ensuring security in the university buildings.
2. The purpose of the measures and requirements applied according to these regulations is
   2.1. to ensure the safety and security of persons staying in the buildings;
   2.2. to ensure the protection of the university’s property and information in the case of theft or attack;
   2.3. to eliminate potential accidental damage to the university’s property and information.
3. The regulations are implemented in accordance with national legislation and bylaws resulting from national legislation.
4. The conditions and requirements established by and based on the regulations must also be observed upon planning construction works in the university buildings and rooms and upon ordering and completion of building design plans.
5. For guarding the buildings and protecting the people and assets in the buildings, the university uses physical protective equipment, electronic security systems and, if necessary, manned guard (‘security systems’), and guidelines for conduct established based on the regulations.
5¹ For the purposes of the regulations, the head of a structural unit is head of institute, director of college, director of non-faculty institution of the university, head of the dean’s office and head of support unit. [effective as of 7 January 2016]

II. Security concept for buildings

6. Head of Estates Office approves the security concept for each building of the university based on proposals made by head of the structural unit that uses the building, head of in-house security service, building superintendent and security systems specialists, taking into consideration the needs of the users and the specifics of activities conducted in the building, part of the building or room.
7. The security concept specifies
   7.1. the division and description of the building’s security levels;
7.2. restrictions on movement in and access rights to the building, parts of the building and rooms at each security level;
7.3. the conditions for arming the security system in the building and its parts, incl. rooms;
7.4. the principles of using manned guard in the building;
7.5. other important security conditions of the building.

III. Measures for ensuring security

8. Physical protective equipment includes doors, locks, security roller shutters, security trellis barriers, high-security glass panes and structural elements and safety films.
9. Electronic security systems used by the university in its buildings include an automatic fire alarm system, technical or electronic security system, access control system and video surveillance system.
10. Manned guard is generally placed in a building which is daily used by more than 600 students and employees, and in which due to the size or intended purpose of the building it is necessary to help people find rooms and/or control people’s movement in the building.

IV. Requirements for security systems

11. The security system of a building must be designed for prevention of a threat or attack and this presumes a multi-tiered structure of security requirements both in the grounds and in the building as a whole.
12. For the implementation and control of the security systems, the director of administration establishes in a directive
   12.1. the technical requirements for security systems and the requirements for passive protective equipment and electronic security systems;
   12.2. the procedure for arming the security systems in buildings and rooms;
   12.3. the procedure for keeping, ordering, issuing and using keys.
13. Security systems must be as simple and convenient to use as possible and the technical equipment of security systems must be as unnoticeable as possible.
14. When planning security systems, the university prefers technical guarding to manned guard, and solutions that help to save on the fixed costs of the building.
15. The planning, designing, building and implementation of security systems is coordinated by Estates Office (head of in-house security service, security systems specialists, building superintendent) in cooperation with heads of the structural units that use the building.
16. When planning, designing and changing security systems, the intended use and specifics of the building and the needs of its users must be taken into consideration, and particular attention must be paid to the issues of protecting persons in the building.
17. When designing and building new structures or renovating the existing buildings or parts of buildings, contactless access control systems are preferred for security considerations.

V. Building security levels

18. The university buildings may have up to three zones of different security levels – an open access area and limited access areas of two levels.
   18.1. An open access area is called the green area.
   18.2. Limited access areas are called, depending on restrictions imposed on access to the area, either yellow or red areas.
19. The division of a building and its parts into different security levels is prescribed in the security concept of each building.

20. The building is divided into guarded areas (groups of rooms) and access control groups, taking into consideration the organisation of work in the building, by the building superintendent, head of in-house security service, senior specialist for security systems of Information Technology Office and a person appointed by head of the structural unit that uses the building, working in cooperation. If they cannot reach a common position, head of in-house security service will decide the division of the building into guarded areas and access control groups.

21. The green area is an open area, which may be accessed by students, employees and visitors during the opening hours of the building. The green area includes general auditoriums, cafes, foyers and other public rooms, and also administrative and office rooms in daytime hours specified by users of such rooms, in case the users of the rooms deem it necessary from the aspect of organisation of work that the rooms belong to an open access area.

22. The yellow area is a half-restricted area to which employees working and students studying there have access by means of a contactless access card or a key given for personal use. The yellow area includes administrative and office rooms, auditoriums equipped with presentation and media equipment, academic computing facilities, rooms for utility systems and other rooms to which access by unauthorised persons must be restricted or where their activities must be controlled.

22.1. The yellow area is open for students and visitors during reception hours (during such period it becomes a green area) or if access is granted by means of the entryphone system.

22.2. In the yellow area, equipment of the security system is installed in rooms, and the security system in the rooms is armed according to the terms and conditions established herein and pursuant to the regulations of guarding buildings and rooms.

22.3. Equipment of access control system is installed in front of entrances to rooms or parts of the building.

22.4. University employees and students who are not authorised to access the yellow area and visitors are allowed to enter the yellow area only if accompanied with a person who works in the yellow area.

23. The red area is an area to which access is allowed only with the employee’s personal access card (employment certificate). Other persons are allowed to access the area only if accompanied by an employee of the university. The red area includes, for example, laboratories equipped with high-tech tools and equipment, special high-risk laboratories, server rooms, archives, repositories and other rooms of increased security risks.

23.1. Entrances to areas or rooms are visually monitored and electronically guarded by means of the video surveillance system.

23.2. In the red area, the equipment of access control system is installed in front of the entrances, the equipment of the security system is installed in the rooms, and the security system in rooms is armed according to the terms and conditions established herein and pursuant to the regulations of guarding buildings and rooms.

24. If the structural unit has in their possession valuable and/or important equipment, which the head of the structural unit wants to guard separately, the head of the structural unit notifies the security control service thereof. In cooperation with in-house security service, the possibilities and conditions for guarding the equipment are agreed upon.

VI. Terms and conditions of arming security system in buildings and rooms

25. The security system in rooms and parts of the building must be armed by employees who use them. In a room or part of the building which forms a common guarded area, the last employee to leave the room or part of the building must arm the security system. If a room is disarmed, the security
person of the building or the security control centre is entitled to arm the security system in the
room.
26. An employee who leaves a room or part of the building must upon leaving the room at the end of
the working day lock the doors, close the windows, turn off the lights, switch off electrical
equipment (except equipment that requires permanent power supply, e.g. refrigerators etc.), ensure
that in rooms equipped with IT equipment (special equipment, multimedia devices, computers etc.)
the equipment is switched to sleep mode according to the user manual or the procedure established
in the university, and in case a security and alarm system is available in the rooms, arm the system.
26.1. The same must be done in rooms given for temporary use by the person in charge of
using the rooms at the end of using the rooms.
26.2. The key(s) to the room(s) must be returned to the building security person or
receptionist or left in a designated place (e.g. in a key cabinet).
27. If the person who is the last to leave the room fails to perform the obligations specified in clause
26, the employee bears proprietary liability for causing damage to the employer pursuant to
employment contract, contract of proprietary liability and bylaws. A person temporarily in charge
of the rooms is liable pursuant to the contract or other agreements they have made.
28. Before entering a working room, the employee must ensure that rooms are not armed and if
necessary, disarm the system in the rooms. A cleaner of the building or room disarms and arms the
system only in his or her assigned cleaning area, using a personal security code.
29. Open entrance to the building is guaranteed at times specified in the security concept of the
building. Entrance with an access card is applied at times specified in the security concept of the
building.
30. The security system in the whole building is generally armed at 23:00 every working day, and on
weekends and public holidays at times specified in the security concept of the building.

VII. Terms and conditions for access to and movement in buildings and rooms

31. Employees can access their workplace using an access card, security code and/or key. An access
card or employment certificate must be carried along and presented to the receptionist or the
security person of the building at their first request.
32. After signing an employment contract, an employee is entitled to get an employment certificate (a
plastic card with a photo), which can also be used as an identification and access card functioning
as an electronic key and ensuring access to the building, room(s) and/or workplace that is
necessary for the employee to perform the duties.
33. If a student needs access to a building, part of a building or room, an access card is issued to the
student by the building superintendent based on the proposal of the academic affairs specialist.
34. Giving, amending and terminating access rights to working rooms and auditoriums is organised by
the building superintendent based on an application submitted by head of structural unit or a person
appointed by head of the structural unit that uses the building or part of the building. The
application must be in a format which can be reproduced in writing. A proposal to give access
rights to an employee is made by the employee’s immediate supervisor. The right to use
auditoriums equipped with an access control system is given to an employee using the auditorium
based on information entered in the study information system.
35. Main entrances to administrative buildings are open during daytime, generally from 7.00 to 17.00.
In academic buildings in which studies are conducted, the main door to the building is open at
times communicated to the security control centre by the faculties, generally from 7.00 to 18.00.
36. If the main door of the building is closed, only persons with access rights are allowed to enter the
building with their access card.
37. The front door of the building is kept open and access to the place of conducting studies is
guaranteed pursuant to information communicated to the university security control centre by each
faculty. For that purpose, a person appointed by the faculty must inform the university security control centre of times when studies are conducted in the building, primarily of times of studies that take place on weekends and on working days after 18.00. If the times of studies in the building change, the faculty’s academic affairs specialist must inform the university security control centre of such changes. If the security control centre has not been notified of the changed times of studies, the security control centre keeps the entrance to the building closed.

38. On working days from 23.00 to 06.00 and on weekends and public holidays from 20.00 to 08.00 people are not generally allowed to stay in the building. If a person who holds access rights to the building stays in the building or leaves the building, incl. for performance of urgent duties, during the said times, the person has to give advance notice to the security person of the building, or in the absence of such officer, the university security control centre. On weekends and public holidays from 8.00 to 20.00 the principles specified in clause 36 are applied.

39. One must not stay in limited access rooms without the presence or consent of persons working there. An employee may enter a limited access room and area only if accompanied by an employee who has access rights to the room or area.

40. Employees with a right to enter limited access rooms or areas (primarily the yellow area) must ensure that a person entering at the same time with them has the respective access rights. The university security control centre must be immediately notified of any unauthorised entry by phone at 737 5111 (5111). Employees with a right to enter limited access rooms may take non-work-related visitors into the rooms with them only if allowed by head of the structural unit possessing the rooms or immediate supervisor. An employee who has allowed a visitor to enter a limited access area is responsible for the visitor’s actions in the area.

41. Students are generally authorised to access an auditorium for the time of studies either with the permission of an employee with access rights to the auditorium or pursuant to the lecture plan entered in the study information system.

42. In limited access rooms of the yellow area which are open for students for independent work (e.g. computer classrooms), manned guard or electronic surveillance of the equipment must be provided.

43. The person appointed by head of Estates Office must be immediately informed of the termination of employment contract with an employee.

44. The emergency evacuation doors of a building must be closed at all times and the security armed. Evacuation doors must not be opened for any other purposes than evacuation from the building.

45. An employee or a student must inform the university security control centre of the loss of an employment certificate or access card by phone at 737 5111 (5111).

VIII. Conditions of keeping, ordering, issuing and using keys

46. An employee is responsible for the key issued to him or her.

47. Permission to access the workplace and get a personal key to the working room is given by the employee’s immediate supervisor, who presents a duly completed application form to the building superintendent. The building superintendent issues the key to the employee against signature. The employee must use the key solely by him- or herself and must not hand over the key to other persons.

48. Keys to public rooms of the building and auditoriums are issued by the receptionist of the building only to persons who hold access rights to these rooms pursuant to the lecture plan entered in the study information system or rights given by the head of the structural unit that possesses the rooms.

49. After using the public rooms and auditoriums, the person who received the key must return it to the key cabinet or to the receptionist of the building.

50. Upon losing the key the employee must immediately inform the building superintendent.
51. The forms of the application for issue of keys, the application for staying in the building at night-time and the application for getting access rights to rooms are developed by the head of Estates Office.

IX. Liability

52. The everyday use, application and maintenance of security systems in buildings located in the city of Tartu is ensured by the building superintendent in cooperation with the university security control centre and the in-house security service of Estates Office.

52.1. The guarding and protection of buildings and property is guaranteed in cooperation with the in-house security service of Estates Office and the university security control centre and the security company operating based on a contract for services.

52.2. The guarding and protection of buildings is organised and managed around the clock by the university security control centre, whose operation is coordinated by head of the in-house security service.

53. The everyday use, application and maintenance of security systems in buildings located outside the city of Tartu is ensured by head of the structural unit that uses the building or a person appointed by head of the structural unit.

54. Estate Office makes the security concepts specified in clause 7 and the forms of applications specified in clause 51 available on the intranet.

55. The director of administration will bear responsibility for the performance of these regulations.

X. Implementation provisions

56. The regulations take effect on 1 July 2011.