Consolidated version
the document is informative in nature

The decision of the Senate "On the approval of the security policy of Riga Technical University" was approved at the meeting of the Senate on April 28, 2014 (protocol No. 580), with amendments:

- on May 26, 2014 (entered into force on May 27, 2014);
- May 27, 2019 (entered into force on May 28, 2019)

About the approval of the security policy of Riga Technical University

Taking into account the need to establish RTU security guidelines, as well as to ensure internal processes and environment to protect RTU staff, visitors, cooperation partners, material and intangible assets of RTU from external and internal threats, as well as based on Article 44 of the RTU Constitution, which stipulates : " ... *The Senate approves the procedures and regulations that regulate all spheres of RTU activity* ", **the RTU Senate decides:**

1. Approve RTU's internal normative act " Security Policy of Riga Technical University" (hereinafter - Policy);

2. Determine that the activities related to the implementation of the RTU Policy are ensured by the following RTU structural units/employees in accordance with their competence:

2.1. security - a structural unit related to security or a structural unit that coordinates the activity of the outsourcing service provider;
(expressed in the version approved at the Senate meeting on May 27, 2019)

2.2. occupational safety and civil protection, compliance with fire safety measures and information technology environmental safety - Administrative Service ;
(expressed in the version approved at the Senate meeting on May 27, 2019)

2.3. security of financial and related protected information – Financial Vice-Rector's Service ;
(expressed in the version approved at the Senate meeting on May 27, 2019)

2.4. information related to intellectual property of RTU - Office of the Vice-Rector of Sciences;
(expressed in the version approved at the Senate meeting on May 27, 2019)

2.5. environmental security of information technology - Department of Information Technology ;
(expressed in the version approved at the Senate meeting on May 27, 2019)

2.6. security of publicly available and restricted information – Document Management Department ;
(expressed in the version approved at the Senate meeting on May 27, 2019)

2.7. RTU employees appointed in accordance with the rector's order are responsible for the protection of state secrets, the classified information of the North Atlantic Treaty Organization, the European Union and foreign institutions .
(expressed in the version approved at the Senate meeting on May 27, 2019)

3. To authorize the rector by order to determine the actions related to the implementation of " Riga Technical University's security policy" to the responsible persons and structural units , including, but not limited to, the development of internal regulatory acts, risk assessment, etc.

Security policy of Riga Technical University

Issued under
Article 44 of the Riga Technical University Constitution

I. Terms used

1.1 . Security is a state achieved as a result of unified, targeted measures implemented by the RTU, in which internal and external threats cannot cause significant damage to the operation and development of the RTU.

1.2. A threat is a source of harm that negatively affects or may affect RTU, RTU staff, visitors or cooperation partners.

1.3. Objects of danger are movable and immovable property owned or used by RTU (including but not limited to buildings, land, etc.), intellectual property, databases, restricted access information, etc.), personal life and health.

1.4. Internal security threats are sources of damage that may occur in RTU as a result of the actions or inactions of any RTU staff member (eg, fire, accidents in internal engineering networks, etc.).

1.5. External security threats are such sources of damage that may occur due to *force majeure majeure*) (e.g., flood, earthquake, etc.) or as a result of the action or inaction of third parties (e.g., theft, illegal access to the server, etc.).

1.7. An information system is a computerized system of data entry, storage and processing, which provides for user access to the data or information stored in it.

1.8. The internal security system is a set of organizational and technical security measures that ensure the prevention or reduction of the probability of occurrence of threats and the damage caused by them, the ability to warn about threats in time, counter them and prevent their consequences.

II Policy objective and guidelines

2.1. The policy has been developed and is implemented in accordance with the legal norms in force in Latvia.

2.2. The purpose of the policy is to ensure such internal processes and environment that RTU's staff, visitors, cooperation partners, RTU's tangible and intangible values are protected from external and internal threats, as well as to ensure RTU's operation and development in line with RTU's regulatory enactments and the goals set in RTU's strategy.

2.3. The policy defines general principles of organization and implementation of RTU's internal security system.

2.4. RTU recognizes the life and health of a person as the primary object of threat to be protected.

2.5 . The RTU provides permanent funding in the RTU budget to ensure the reduction and/or prevention of the impact of RTU threats.

III Safety management system

3.1. RTU is obliged to provide RTU staff with an accessible and clear description of the internal security system, including, but not limited to, internal regulatory acts regulating security, document forms and a list of persons or structural units responsible for security available on the internal website ORTUS.

3.2. In accordance with the purpose of this policy, RTU organizes and maintains an internal security system that includes:

3.2.1. internal security monitoring, including regular security risk assessment;

3.2.2. the person(s) or structural units responsible for security subordinate to the rector;

3.2.3. base of internal regulatory acts;

3.2.4. informing staff about security-related issues and creating feedback.

3.3. The internal security system of the RTU ensures the following functions:

3.3.1. taking preventive actions to reduce threats;

3.3.2. RTU personnel education in security issues;

3.3.3. timely warning of potential threats;

3.3.4. protection and response to threats and prevention of their negative effects;

3.3.5. mitigation of the negative consequences caused by the realization of threats.

3.4. While in the building owned or used by RTU or in the plot of land, each person is primarily responsible for the safety of himself and the things in his possession or responsibility.

3.5. If necessary, but not less often than once every 2 (two) years, based on the rector's order, an audit of the internal security system or its component is conducted.

3.6. The purpose of the audit is to check the compliance of the security system or its part with the valid external and internal regulatory enactments of the RTU, to identify the shortcomings related to the security system and to report to the management of the RTU about recommendations for the elimination of the shortcomings.

IV Environmental and physical security

4.1. RTU implements physical protection measures that reduce internal and external security threats (e.g. fire, flood, collapse, theft, personal injury, etc.).

4.2. RTU's internal regulatory acts determine the internal rules of procedure for RTU students and employees, including, but not limited to, rules for activities in auditoriums, laboratories, libraries, service hotels, etc. in RTU premises.

4.3. RTU appoints occupational safety specialists responsible for work safety at RTU. At the same time, a trusted person(s) trained in accordance with the procedures established by the Cabinet of Ministers, who represents the interests of employees in labor protection , is elected and operates in accordance with regulatory enactments in RTU structural units .

V Security of material values

5.1. All material values of RTU are listed and inventoried in accordance with the requirements of regulatory acts.

5.2. RTU concludes an agreement with the employee, with whom the employee accepts the material values of the relevant structural unit as material responsibility and who is responsible for their safety.

5.3. RTU employees are personally responsible for the safety of material assets that are in their responsible use (e.g. laboratory dishes, computers, etc.). The mentioned material values may be located outside the RTU, if agreed with the head of the structural unit.

VI Information security

6.1. The procedure for the circulation of generally available and restricted information in RTU is determined by external and internal regulatory acts of RTU.

6.2. RTU provides an information technology environment that protects information resources against external and internal security risks, as well as ensures continuous and high-quality operation of RTU. The rules related to the security of the information technology environment are determined in the RTU's internal regulatory act, a specially appointed employee with the appropriate qualifications - the information systems security manager - is responsible for the security management of the RTU's information system.

6.3. RTU ensures the conclusion of an agreement/agreement on non-disclosure of information with those RTU staff members (e.g. with researchers in laboratories) and/or third parties who are connected or may be connected in the future with information, the disclosure of which would harm the interests of RTU.

6.4 . RTU is obliged to conclude a non-disclosure agreement/agreement with persons whose official duties are related to restricted access information, the disclosure or loss of which, due to the nature and content of this information, hinders or may hinder the operation of RTU, causes or may cause damage to the legal interests of persons.