Consolidated version
the document is informative in nature

The Security Policy of Information and Communication Technology Systems of Riga Technical University was approved at the Senate meeting of June 27, 2016 (protocol No. 601), with amendments:

- December 27, 2021 (entered into force on December 28, 2021)

Security Policy of Information and Communication Technology Systems of Riga Technical University

Issued on the basis of RTU Senate 28.04.2014.
of the decision " Safety of Riga Technical University
policy " (protocol No. 580) subsection 6.2

I. General questions

1. The information systems security policy of Riga Technical University (hereinafter - RTU) defines the guidelines for the management of information systems, which ensure the safe use of RTU's information systems by implementing and maintaining a sufficient set of measures to reduce or prevent potential or caused damage.
2. The policy applies to RTU's information and communication systems (hereinafter - Systems), which are registered in the Systems Register approved by order of RTU Rector, as well as the infrastructure of information and communication systems related to it.

(expressed in the version approved at the Senate meeting on December 27, 2021)

3. System security management is organized in accordance with the principle of proportionality, where the costs of implemented security measures do not exceed the losses incurred as a result of potential damage.

II. Terms used in politics

4. System - is a set of internal and external information and technical resources that is created, works and is maintained to collect, accumulate, process, store and use information.
5. System user – a natural person who uses the System in accordance with the contract concluded with RTU.
6. System Security Manager (hereinafter – Security Manager) – a person who implements System Security Management at RTU.
7. Information resource – data files, databases, archives, etc. resources that are processed, transmitted, stored or perform other functions, regardless of the type of data carrier.
8. Technical resource – computers, network hardware, communication lines and other technical means used for information processing, transmission and storage.
9. Resource holder – the head of the RTU structural unit to which the specific System is linked in the Systems Register. The holder of the resource carries out the classification of the Systems, the analysis of security risks, the determination of security measures, and also determines the circle of persons who are allowed to access the System.
10. Resource custodian – a person (qualified technical specialist) who performs system administration work, including responsibility for maintaining the System and ensuring the functionality of the corresponding technical resources or some of their parts.
11. The person responsible for the security of the System (s) is a person appointed by the decision of the Senate or the rector's order in the structural unit (s) of RTU.
12. Intrusion Detection/Prevention System – equipment or software that monitors the activities of the Systems with the aim of detecting, preventing or reporting malicious activities.

13. Incident – any action, as a result of which the Security of the Systems is or may be affected.

14. Integrity – preservation of complete and unchanged information .

15. Availability – access to information within a certain period of time after the information is requested.

16. Confidentiality – transfer of information only to those persons who are authorized to receive and use it .

17. Encryption - A way to make data unreadable by anyone except the person who has the proper encryption key to decrypt the data.

18. Technical security measures – a set of protection measures used to ensure a sufficient level of confidentiality, integrity and availability.

III. System security management organization and responsibility

19. The rector of RTU (hereinafter - the rector) appoints the responsible persons for ensuring the security of the Systems.

20. By order, the Rector determines the Security Manager - a person who organizes and manages the implementation of security measures of RTU Systems, in compliance with the requirements set out in the regulatory acts.

21. In case of necessity, the rector determines the person responsible for the security of the System(s) in the RTU structural unit by order in individual structural units.

22. The person responsible for System Security is responsible for the System Security Management in the RTU structural unit and for coordinating their actions with the Security Manager.

23. The Security Manager develops, updates and is responsible for the System classification process and its supervision, as well as maintaining the System register in an up-to-date state.

24. The Security Manager organizes the training of System users on System security issues.

25. System security requirements according to assigned security classes are determined by the resource holder. The resource holder, in coordination with the Security Manager, has the right to set special security requirements for the attached System, as long as they do not conflict with the Policy.

26. The resource holder is responsible for classifying the system, analyzing risks, determining security measures, as well as determining the persons who are allowed access to the System.

27. Heads of RTU structural units are obliged to cooperate with the Security Manager in maintaining the System Register information in an up-to-date state, including informing about the Systems under their control, which should be included in the System Register.

28. The integrity, availability and confidentiality security classes of the systems are reviewed at least once a year, as well as in cases where changes affect the security of the systems.

29. The Internal Audit Department is responsible for organizing and/or conducting System Audits and reporting to the RTU management about the findings during the audit, the risks discovered, their impact on the RTU, and submits recommendations for mitigating the discovered risks, in accordance with the regulations of the Internal Audit Unit.

Characteristics of systems

30. The systems are used to create, collect, accumulate, process, use and destroy information necessary for the performance of RTU functions.

31. The physical protection of systems is provided taking into account their security classes.

IV. System security classes

32. Evaluating the acceptable level of security risks of the System, the holder of the resource assigns it the appropriate security class in accordance with Subsection 7.1 of Cabinet of Ministers Regulation No. 422 of July 28, 2015 "The procedure for ensuring the compliance of information and communication technology systems with the minimum security requirements".

33. If the System is assigned three B security classes or at least one A security class, the System is considered a high security System. In other cases, the System is considered a basic security System.

V. System security risk management

34. The Resource Holder and the Security Manager are responsible for the management of System security risks.

35. System security risk analysis is performed for all high security systems.

36. For basic safety systems, safety risk analysis is performed by evaluating its necessity.

37. System security risk analysis is carried out if changes are planned to be made in the enhanced security system, which affect the security of the system .

38. Systems security risk analysis can be initiated by the Rector, Resource Holder, Resource Custodian or Security Manager.

39. Before the next System security risk analysis, the Security Manager evaluates the System security risk mitigating measures implemented by the responsible employees defined in the System security risk management plan.

VI. Users of the Systems and means of access to the Systems

40. Granting and revocation of System user rights, including registration of new users and revocation of rights in the event of termination of employment or other contractual relations, is carried out by the System holder or manager in accordance with the rules that determine the grant and revocation of user access rights.

41. The holder or manager of the systems introduces the RTU employees, before granting user rights, with the internal regulatory acts of the RTU, which determine the rights, duties and responsibilities of the users of the systems.

42. The rights and obligations of users are determined in RTU's internal regulatory acts or, in accordance with security requirements, in concluded contracts/agreements.

43. Each user of the Systems is assigned an individual identifier and password (at least 9 characters), which must be changed when registering for the first time in the Systems.

44. Each user account is associated with a specific natural person. If the System uses accounts that cannot be linked to the specific natural person, then the System has technical means that prevent users from using these accounts.

45. The user of the systems has access only to those information and technical resources that are necessary for the performance of work duties (the functions of the systems can be performed with the minimum possible rights).

46. For system users whose access rights are based on employment legal relations with RTU, the user's rights are canceled on the day when all employment legal relations agreements between RTU and the System user are terminated. The resource holder has the right to determine special exceptions.

47. Depending on the duties to be performed, System users use special user accounts that are assigned to them.

48. It is prohibited to electronically store and transport data, System user passwords, including those obtained as part of the System user authentication process, in an unencrypted form.

49. At least once a year, the resource holder reviews the access rights of System users under his control.

50. Access of third parties (suppliers, consultants, etc.) to the System (except for public information resources) is implemented in accordance with contractual relations and RTU's internal regulatory enactments.

51. The Security Manager has the right to revoke the user's access rights for non-compliance with the rules of use of the System.

52. The security manager, warning the responsible person (resource guardian) about the IP address (system) or, if it cannot be ascertained, the RTU User Support Center, has the right to disconnect the information system or device from the network, in cases where there are reasonable suspicions that it is being or can be used for malicious activities. An information system or device is connected to the network after the responsible person (custodian of the resource) has taken appropriate actions to prevent misuse of the device.

(added based on the decision of the Senate of December 27, 2021)

VII. Systems development and maintenance

53. System security requirements are identified and documented in each phase of defining the requirements of the project related to the development of the System, by justifying and coordinating them with the resource holder.

54. Operating Systems are separated from development and test Systems by marking them accordingly, and use different user identifiers and passwords from the operating System or, using the same user identifiers and passwords, ensure equivalent security requirements for the test and operating System.

55. The head of the RTU structural unit who ordered the development of the System is responsible for registering the System in the System Register.

56. When ordering the development of the System, it is determined that:

56.1. the source code of the System's computer programs is available and the right to use it is transferred to RTU;

56.2. the period of System maintenance and support provision (including the elimination of System security flaws) has been determined;

56.3. before putting a new System into operation, it has undergone penetration tests.

57. Access to System files (including software source code) is controlled by providing change control and auditing of access attempts.

58. Security features are incorporated into the system for correct data entry and processing.

59. In the system that ensures receipt of electronic mail from external resources, incoming communication is processed at least in accordance with the requirements of the e-mail authentication protocol (DMARC), implementing e-mail processing according to the DMARC policy of the sender's domain name, generating a report and sending it to the contact specified in the DMARC configuration

(added based on the decision of the Senate of December 27, 2021)

60. Default passwords (set by the manufacturer or distributor) are not used for equipment, including infrastructure equipment that ensures the functioning of the System.

61. RTU carries out regular monitoring of software vulnerabilities, ensuring prompt installation of software fixes for both operating systems and other used software.

VIII. Systems security incident management

62. RTU maintains a log of System Security Incidents.

63. Resource Custodians discover and record System Security Incidents in the System Security Incident Log.

64. In case of detection of a system security incident, the Security Manager is informed, who makes a decision on further actions to prevent the incident.

65. All end-user equipment at the RTU used to connect to the System must include anti-virus functionality.

66. RTU uses the Automated Intrusion Detection/Prevention System.

67. RTU is provided with the creation and storage of System Audit records for at least 6 (six) months after the record is made. For Enhanced Security Systems – 18 (eighteen) months after making the entry.

68. Any access to the Systems is traceable to a specific System user account or Internet Protocol (IP) address.

IX. Management of continuous operation of systems

69. Security Manager develops and manages the System's continuous operation plan, assuming that the costs of ensuring the continuity of the Systems' operation must be commensurate with the possible losses that could arise from the interruption of the System's operation.

70. Business continuity measures are focused on RTU's core business process and enhanced security Systems, determining measures that ensure the restoration of processes and services after a significant System incident.

71. Documents related to business continuity are updated, tested and revised after changes are made to the System, or at least once a year.

X. Final question

72. The order in which safe use of Systems is organized at RTU is determined by internal regulations approved by the rector.