

**MINISTRY OF SCIENCE AND HIGHER EDUCATION
OF THE REPUBLIC OF KAZAKHSTAN**

**NON-PROFIT JOINT-STOCK COMPANY
«D. SERIKBAYEV EAST KAZAKHSTAN
TECHNICAL UNIVERSITY»**

APPROVED

by resolution of the Board of
Directors of
NJSC “D. Serikbayev East
Kazakhstan Technical
University”
Minutes No. 7
dated December 25, 2024
(as amended on April 30, 2026,
Minutes No. 6)

**RISK MANAGEMENT POLICY
of NJSC “D. Serikbayev EKTU”**

RMP NJSC “EKTU” 115-I-2024

Contents

1. General Provisions	3
2. Terms and Definitions	3
3. Risk Management Objectives	5
4. Objectives of the Risk Management System	5
5. Limitations of this Policy	5
6. Risk Management Principles	6
7. Infrastructure of the Risk Management Process	6
8. Risk Management Process	11
9. Miscellaneous Provisions	14
Appendix 1 – Risk Classification	15
Appendix 2 – Change Registration Sheet	16

1. General Provisions

1. The Risk Management Policy of NJSC “D. Serikbayev EKTU” hereinafter referred to as the Policy, has been developed in accordance with ISO 31000:2018 “Risk Management — Guidelines”, ISO 9001:2015 “Quality Management Systems — Requirements”, ISO 37001:2016 “Anti-Bribery Management Systems — Requirements with Guidance for Use”, ESG-2015 “Standards and Guidelines for Quality Assurance in the European Higher Education Area”, the Corporate Governance Code of a non-profit joint-stock company in the field of higher and postgraduate education, and internal regulatory documents governing the activities of NJSC “D. Serikbayev East Kazakhstan Technical University” hereinafter referred to as NJSC “EKTU” or the University. This Policy establishes terms and definitions, the goals and objectives of the risk management system (RMS), and its principles; defines limitations and requirements for the infrastructure and process of risk management; and regulates the risk management process at EKTU in relation to risks subject to consideration in order to prevent or reduce their adverse impact.

2. This Policy is available to all interested parties on the University website and is mandatory for all employees of NJSC “EKTU” in the performance of their duties.

3. This Policy does not aim to cover all possible scenarios that may arise in the course of its practical application. It assumes that risk management, as part of day-to-day operations, should allow flexibility in applying different management styles and creative approaches.

2. Terms and Definitions.

4. The following terms, definitions and abbreviations are used in this Policy in accordance with the regulatory documents on the basis of which it was developed:

1) **Automated RMS System** — a specialized web portal, rms.ektu.kz, designed to digitalize risk management processes.

2) **Consequence** — the outcome of an event affecting objectives.

3) **DSDQA** — Department of Strategy Development and Quality Assurance.

4) **Event** — an incident or occurrence with an internal or external source in relation to the organization, which affects the achievement of established objectives.

5) **I** — Instruction.

6) **Key Risks** — major risks included in the Key Risk Register approved by the Board of Directors.

7) **Likelihood** — the possibility that something may occur.

8) **NJSC “EKTU”** — Non-profit Joint Stock Company “D. Serikbayev East Kazakhstan Technical University”.

9) **Residual Risk** — the risk remaining after actions have been taken to change the likelihood or degree of impact of that risk.

10) **Risk** — the effect of uncertainty on objectives; an event that may or may not occur. A risk may be negative, such as loss, damage or harm; neutral; or positive, such as gain, benefit or profit.

11) **Risk Acceptance** — willingness to cover possible losses, for example by establishing special funds and reserves to compensate for losses.

12) **Risk Appetite** — the degree of risk that the University considers acceptable in the process of achieving its objectives.

13) **Risk Assessment** — the overall process of risk identification, risk analysis and determination of the risk level.

14) **Risk Avoidance** — adjusting process management in order either to eliminate the threat posed by a negative risk or to change the objectives of the process affected by the threat.

15) **Risk Criteria** — data against which the significance of a risk is assessed.

16) **Risk Factor** — conditions, states or circumstances under which the causes of risk arise, leading to the materialisation of the risk.

17) **Risk Identification** — the process of finding, recognising and describing a risk.

18) **Risk Management** — a set of methods, techniques and measures that make it possible to forecast the occurrence of risk events and take measures to eliminate or reduce the negative consequences of such events.

19) **Risk Management System** — a systematic approach that enables risks to be identified and managed on a systematic basis.

20) **Risk Map** — a visual and/or textual description of a risk.

21) **Risk Monitoring** — tracking identified risks, monitoring residual risks, identifying new risks and assessing them.

22) **Risk Officers of Structural Units** — responsible employees of the University’s structural units whose duties include organizing risk management activities within their structural units and cooperating with the structural unit responsible for risk management at all stages of implementation of risk management system procedures.

23) **Risk Owner** — a person and/or structural unit responsible for all aspects of managing a specific risk, including reducing the likelihood of the risk materialising and/or reducing the possible impact of the consequences of the risk materialising at NJSC “EKTU”.

24) **Risk Reduction** — reducing the likelihood or consequences of a high-risk negative event to acceptable limits.

25) **Risk Transfer** — redirecting responsibility for responding to the negative consequences of a threat to another party; this is effective for financial risks.

26) **Sole Shareholder** — the Ministry of Science and Higher Education of the Republic of Kazakhstan.

27) **Tolerance Level** — an acceptable level of deviation in relation to the achievement of a specific goal or objective. The tolerance level enables effective monitoring and prevention of exceeding the risk appetite.

3. Risk Management System Objectives

5. The goals of the risk management system are as follows:

1) To build an effective and comprehensive system and establish an integrated risk management process as an element of University governance, as well as to continuously improve activities based on best practices and a unified standardized approach to risk management methods and procedures, in order to ensure the stability of NJSC “EKTU” operations and protect its value from risks.

2) To ensure that the University accepts risks that are appropriate to the scale of its activities.

Risks shall remain within the criteria established by NJSC “EKTU”.

4. Objectives of the Risk Management System

6. The tasks of the risk management system are as follows:

1) To ensure a continuous and coordinated risk management process based on timely identification, assessment, analysis, monitoring and control of risks in order to support the achievement of the established objectives.

2) To implement and improve the risk management system, enabling the prevention and minimization of potentially negative events.

3) To increase the efficiency of resource use and allocation.

4) To prevent losses and damages by improving the efficiency of NJSC “EKTU” activities.

5. Limitations of this Policy

7. The Risk Management Policy is aimed at providing reasonable, but not absolute, assurance that the objectives of risk management will be achieved, for the following reasons:

1) Risk identification and assessment cannot be absolutely accurate due to the uncertainty of future events.

2) Certain risks are beyond the control of NJSC “EKTU” and therefore cannot be fully eliminated.

3) The effectiveness of certain control procedures implemented for risk management purposes may not be achieved due to the human factor.

6. Risk Management Principles

8. The principles of risk management are as follows:

1) Integration.

Risk management is an integral part of all University activities.

2) Structure and Comprehensiveness.

A structured and comprehensive approach to risk management contributes to achieving consistent and comparable results.

3) Customisation.

The structure of the system and the risk management process are customised and aligned with the external and internal environment of the University related to its objectives.

4) Involvement.

Appropriate and timely participation of stakeholders enables their knowledge, opinions and perceptions to be taken into account. This results in increased awareness and a more informed approach to risk management.

5) Dynamism.

Risks may emerge, change or disappear as the external and internal environment of the University changes. Risk management anticipates, identifies, confirms and responds to these changes and events in a timely and appropriate manner.

6) Best Available Information.

Inputs to risk management are based on historical and current information, as well as future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information shall be timely, clear and available to relevant stakeholders.

7) Human and Cultural Factors.

Human behaviour and culture have a significant influence on all aspects of risk management at every level and stage.

8) Continual Improvement.

Risk management is continually improved through learning and experience.

7. Infrastructure of the Risk Management Process

9. The infrastructure of the risk management process describes the organizational structure of the RMS and establishes the functions and responsibilities of its participants.

In accordance with the principle of involvement, the governing bodies and structural units of NJSC “EKTU” are involved in risk management. Each employee shall ensure that risks are duly considered when making decisions. Managers at all relevant levels are responsible for the development, documentation, implementation, monitoring and improvement of the risk management system in accordance with their functional duties.

10. Based on information submitted by the Board of Directors and/or the Executive Board of the University, **the Sole Shareholder** makes strategic decisions for the purposes of managing the University’s risks.

11. **The Board of Directors** of the University plays a key role in overseeing the RMS and performs the following functions:

- 1) defining the long-term and short-term goals and objectives of the University’s activities;
- 2) approving the organizational structure of the University that meets its needs and ensures adequate control and risk reduction;
- 3) approving the Risk Management Policy;
- 4) approving levels of responsibility for risk monitoring and control by approving this Policy;
- 5) reviewing the conclusions of external auditors on improving internal control and risk management, as well as the results of audits conducted by the Internal Audit Service of the University;
- 6) reviewing reports on the effectiveness of the risk management system;
- 7) monitoring activities through authorized committees established under the Board of Directors;
- 8) approving the risk appetite, the **Key Risk Register**, the Risk Map, and the University’s Risk Management Action Plan.

12. In order to effectively perform the assigned functions, authorized committees may be established under the Board of Directors of the University, the functions of which shall be determined by the relevant regulatory documents.

13. **The Audit Committee** of the Board of Directors of the University performs the following functions in relation to risk management:

- 1) reviews reports of external and internal auditors on the status of the RMS;
- 2) reviews the effectiveness of the University’s RMS tools and provides recommendations for their improvement;
- 3) monitors the implementation of recommendations issued by the University’s internal and external auditors in relation to the risk management system;
- 4) holds regular meetings with the University management to review key risks, control issues and the University’s relevant risk management plans;
- 5) gives preliminary approval to documents and materials, including the Policy, reports and other materials, submitted for consideration and/or approval by the Board of Directors of the University.

14. **The Executive Board of the University** is responsible for organizing an effective risk management system to ensure the implementation of and compliance with the University’s internal regulatory documents. The Executive Board is responsible for developing a sound risk management culture at the University.

The Executive Board of the University performs the following functions:

- 1) implementing the goals and objectives set by the Board of Directors of the University;
- 2) implementing and ensuring compliance with the provisions of this Policy and other internal risk management documents;
- 3) reviewing and submitting reports and other documents to the Board of Directors of the University in accordance with the approved regulatory documents;
- 4) organizing an effective risk management system that enables potential risks to be identified, assessed and managed;
- 5) approving risk response measures within the framework of regulatory documents approved by the Board of Directors;
- 6) approving and improving internal procedures and regulations in the field of risk management;
- 7) approving risk management documents of the University that do not fall within the competence of the Board of Directors of the University.

15. The Executive Board of the University may perform part of its risk management functions through the establishment of relevant committees, whose functions and powers are defined by the relevant regulatory documents.

16. Responsibility for risk management at NJSC “EKTU” is assigned to the Chairman of the Executive Board — Rector. Responsibility for risk management includes, at a minimum:

- 1) establishing and/or appointing risk owners responsible and authorized to manage risks;
- 2) establishing other responsibilities of employees at all levels of NJSC “EKTU”;
- 3) appointing a person responsible for coordinating risk management;
- 4) responsibility for holding regular risk meetings and maintaining relevant reporting;
- 5) responsibility for the achieved results of risk management.

17. **The structural unit** responsible for risk management performs the following functions:

- 1) organizing and coordinating the process of identifying and assessing the University’s risks, as well as controlling and monitoring the implementation of measures to improve the University’s RMS, based on recommendations of the Board of Directors and/or the Executive Board;
- 2) analyzing regulatory and other documentation in the field of risk management;
- 3) developing methodological documents in the field of risk management and providing methodological support to process owners and employees in the identification and documentation of risks, implementation, monitoring and improvement of control procedures, development of risk response action plans and action plans for improving the risk management system, as well as reports on their implementation;
- 4) developing, implementing and improving the methodological framework, policies and rules for risk management and risk monitoring;

- 5) monitoring compliance by the University’s structural units with internal RMS documents;
- 6) reviewing risks of **structural units**, determining risk treatment methods and approving risk management action plans;
- 7) maintaining risk management documentation in accordance with clause 23;
- 8) preparing and submitting risk management reports and other requested information of the University to the Executive Board and the Board of Directors of the University at least once per quarter;
- 9) participating in the organization of periodic assessment of the University’s RMS, and submitting proposals on risk-related matters as part of the assessment of corporate governance and the maturity level of the RMS;
- 10) ensuring the integration of risk management into other processes and developing a risk management culture at the University;
- 11) ensuring automation of the risk management process at the University;
- 12) organizing annual training for University employees on practical aspects of risk management;
- 13) interacting with the Internal Audit Service of the University by providing the Risk Map and **other risk documentation** for the preparation of the internal audit plan by the Internal Audit Service, exchanging information, requesting and discussing audit results in terms of the University’s exposure to risks, and exchanging the database of materialised risks, knowledge and methodologies.

18. In order to avoid conflicts of interest, the head of the structural unit responsible for risk management shall not act as a risk owner, thereby ensuring independence and objectivity.

The head shall not combine this role with functions related to economic planning, corporate finance, treasury, investment activities or internal audit. Combination with other functions is permitted, provided that no significant conflict of interest arises.

19. The responsibilities and powers of the structural unit responsible for risk management are provided for by this Policy and the Regulations on the structural unit.

20. **The Internal Audit Service** of the University performs the following main functions in the risk management process:

- 1) assessing the sufficiency and maturity of RMS elements for effective risk management, including goals and objectives, infrastructure, process organization, regulatory and methodological support, interaction of structural units within the RMS, and reporting;
- 2) assessing the completeness of risk identification and the correctness of risk assessment by the executive body at all levels of its management;
- 3) assessing the effectiveness of control procedures and other risk management measures, including the effectiveness of the use of resources allocated for these purposes;

4) analyzing information on materialised risks, including violations identified as a result of internal audits, cases of failure to achieve established objectives, and cases of litigation.

21. **Structural units** acting as risk owners play a key role in the risk management process and are responsible for:

- approving and implementing the work plan of the structural unit, including measures for managing the risks under their supervision;
- timely identification of risks and informing the structural unit responsible for risk management of significant risks within their area of activity.

22. **Structural Units.** Risk Officers of Structural Units shall be appointed annually by order of the Rector. Their duties include, among others:

- 1) identifying and assessing the risks of the structural unit on an annual basis, with regular review;
- 2) participating, within their competence, in the development of methodological and regulatory documentation on risk management;
- 3) preparing risk management measures jointly with risk owners, monitoring their implementation, and providing regular reports on their implementation;
- 4) timely submission of information on all materialised risks to the structural unit responsible for risk management;
- 5) monitoring external and internal factors that may potentially lead to changes in previous risk assessment results, and submitting relevant information to the structural unit responsible for risk management;
- 6) facilitating the development of communication and risk management culture at the University.

23. The following documents shall be developed and maintained to ensure the functioning of risk management:

- 1) this Policy;
- 2) Regulations on the structural unit responsible for risk management;
- 3) Risk Management Instruction of NJSC “D. Serikbayev EKTU”;
- 4) Key Risk Register of NJSC “D. Serikbayev EKTU” for the academic year;
- 5) Risk Management Action Plan of NJSC “D. Serikbayev EKTU” for the academic year;
- 6) Report on the implementation of the Risk Management Action Plan of NJSC “EKTU”, prepared on a quarterly basis;
- 7) Risk Map of NJSC “D. Serikbayev EKTU” for the academic year.

24. In accordance with the principle of integration:

- 1) Risk management shall be mandatorily embedded into the processes of strategic planning, budgeting, procurement and changes in activities.
- 2) Integration means the continuous use of risk management results in processes, including in process documents such as strategies, budgets, policies, calculations and plans.

3) Relevant plans shall be developed when implementing and improving the risk management infrastructure.

4) The effectiveness of risk management, including both the risk management infrastructure and the risk management process, shall be assessed at least once a year by the Internal Audit Service as part of monitoring.

8. Risk Management Process

25. The University determines the risk appetite it is prepared to accept in order to achieve its strategic objectives. Risk appetite affects the allocation of resources, the organization of processes, and the development of the internal infrastructure within the University required for risk monitoring and response.

Table 1 — University Risk Appetite Recommended

Risk Group		Acceptable Risk Appetite	Explanation
External		High	The University accepts the risks of this group.
Internal	Financial	Medium	The University may accept minor financial risks where necessary, but shall limit its response to them by using available resources.
	Reputational	Medium	The University shall strive to prevent reputational damage and loss of competitiveness.
	Corruption	Low	The University shall not tolerate non-compliance with established legal and regulatory requirements in the field of anti-corruption.

The following tolerance level ranges are established for risk appetite:

- 1) 1-7 – low risk;
- 2) 8-16 – medium risk;
- 3) 17-25 – high risk.

Where necessary, the acceptable risk appetite and tolerance levels may be reviewed.

26. The risk management process consists of:

- 1) risk analysis, including risk identification, calculation and assessment;
- 2) risk treatment, including determination of the treatment method, development, identification of funding sources and implementation of the Action Plan, followed by monitoring of its implementation;
- 3) risk reporting;
- 4) monitoring and revision of the risk management infrastructure and process.

27. The principles of risk management at NJSC “EKTU” in implementing the process are as follows:

Risk Identification.

1) Risks at the University are divided into internal and external risks. The risk classification is provided in Appendix 1.

2) Risk identification shall be accompanied by a description of risks for further analysis. Each risk shall be assigned a number consisting of the Latin letter R and an Arabic numeral, for example, R1.

3) Both risks that the University controls and risks that it cannot control but that affect its activities shall be identified.

4) Priority shall be given to identifying risks at an early stage of their occurrence.

5) When identifying risks, the broadest possible range of consequences shall be considered; however, priority shall be given to the potential impact on the reputation and image of EKTU, capitalization, compliance with regulatory requirements, cost of services, and continuity of operations, where such impact may be estimated in monetary terms.

6) Not only negative but also positive risks shall be identified. Positive risks are understood as risks associated with decisions not to use favourable opportunities.

7) In exceptional cases, where significant changes in the internal or external environment of the University are identified, including as a result of inspections, audits, instructions from government authorities or management decisions, structural units may initiate consideration of the inclusion of new risks.

Such risks shall be subject to additional identification and assessment by the structural unit responsible for risk management.

Where necessary, amendments to the Key Risk Register, the Risk Map and/or the Risk Management Action Plan shall be initiated.

The updated package of documents shall be submitted for consideration and approval by the Board of Directors of the University in the established manner.

Risk management documents affected by such changes and not falling within the competence of the Board of Directors shall be approved by the Executive Board of the University.

Risk Calculation. The following scales shall be used for risk calculation:

1) for calculating likelihood:

Low / Medium / Above Medium / High / Very High;

2) for calculating damage:

Insignificant / Low / Medium / Significant / Catastrophic;

3) risks shall be calculated using expert, stochastic and statistical methods. The preferred calculation method shall be the statistical method.

Risk Assessment.

1) Risks shall be assessed separately by structural units. Each structural unit shall enter the final consolidated list of risks and the results of their assessment into the automated RMS system.

2) The risk manager shall export the final table of structural unit risks from the automated RMS system and determine the arithmetic mean level of key risks and their compliance with the tolerance level and risk appetite.

3) Risks shall be ranked according to the assigned values. Based on the results of risk assessment, each risk shall be assigned one of three values: low, medium or high.

4) For ease of perception, a **Risk Map** shall be prepared for the purpose of reviewing risks at meetings of the Executive Board and the Board of Directors.

Risk Treatment. When considering risk treatment methods, the following treatment options shall be considered:

1) avoiding the risk by deciding not to start or continue the activity that gives rise to the risk;

2) accepting or increasing the risk in order to use a favourable opportunity;

3) removing the source of the risk;

4) reducing the likelihood;

5) changing the consequences;

6) sharing the risk with another party or parties, including through contracts and risk financing;

7) consciously retaining the risk.

28. Risk management measures may be aimed at addressing the causes and factors of risks in order to prevent them, preventive measures, or at eliminating the consequences of a materialised risk. Preventive measures shall be the preferred type of measures.

29. Risk treatment plans shall be documented in the form of a Risk Management Action Plan. Where the Action Plan requires financing, the source of financing shall be determined during its preparation, review and approval.

The Action Plan shall include only project-type measures, that is, measures that have a deadline, a budget and a responsible person, the risk owner.

The cost of implementing a measure for each risk shall be significantly lower than the losses from the risk, taking into account the likelihood of its occurrence. Where measures for critical risks are comparable in cost to the expected losses from the risk, taking into account its likelihood, the need to implement such measures shall be considered by the Board of Directors.

Measures included in the Risk Management Action Plan shall be treated as priorities when preparing the University’s public procurement plan.

30. Risk reporting shall be reviewed at the level of the Board of Directors and the Executive Board on a quarterly basis.

The reporting format shall be determined by the users of the reports and formally approved.

31. Risk Management Monitoring. The structural unit responsible for risk management shall monitor risk management, including assessing:

1) achievement of results;

2) adequacy of the procedures used;

3) adequacy of the information used.

The monitoring results shall serve as input information for risk identification and reporting to the Executive Board and/or the Board of Directors.

Monitoring of the Risk Management Infrastructure and Process.

The structural unit responsible for risk management shall assess the risk management infrastructure and process at least once a year.

Based on the monitoring results, changes shall be made, where necessary, both to the risk management infrastructure and to the risk management process.

9. Miscellaneous Provisions

32. The Risk Management Policy shall be approved by resolution of the Board of Directors.

The Policy shall be reviewed at least once every three years. Amendments to the Policy may be initiated by any members of the Board of Directors and the Executive Board, the Chairman of the Executive Board — Rector, as well as the heads of the Internal Audit Service and the structural unit responsible for risk management.

Appendix 1

Risk Classification



