Approved by
Chairman of the Board, Rector of
Abylkas Saginov Karaganda Technical University NJSC
_____ S.S. Sagintayeva
Board decision
No. 23 dated January 14 2026

INTERNAL REGULARITY DOCUMENT

RULES OF CONDUCTING INTERNAL INFORMATION SECURITY AUDITS

IRD II-03-2026

Developed by: Information security engineer
D.K. Chityan_____

Karaganda

Contents

1 Scope 3
2 Regularory references 3
3 Terms, definitions and abbreviations 3
4 Responsibility and authority 4
5 General provisions 4
6 Procedure for conducting internal audit 5
7 Criteria of the ISMS quality 6
8 Coordination, approval and implementation 6
9 Safekeeping 7
10 Procedure for revising and updatingи 7
Appendix 1 8
Appendix 2 9
Appendix 3 10
Appendix 4 11

1 Scope

1.1 These Rules of conducting internal audits of the information security management system of Abylkas Saginov Karaganda Technical University NJSC have been developed in accordance with the requirements of national and international standards in the field of quality management and information security, as well as the University internal regulatory documents.

1.2 This document defines a unified approach to organizing, planning, conducting, and documenting internal audits of the ISMS within the established scope of the information security management system.

1.3 The requirements of these Rules apply to all the structural divisions, information systems, processes, and University employees involved in the functioning of the ISMS. Compliance with the Rules is mandatory for managers, auditors, and auditees.

1.4 These Rules apply to scheduled and unscheduled internal audits, as well as to analyzing the effectiveness and compliance of the ISMS with established requirements. The internal audit process is considered a continuous element of the functioning of the ISMS and is subject to regular improvement.

1.5 These Rules are an internal regulatory document of the University and are subject to revision and updating when regulatory requirements or ISMS processes change.

2 Regulatory references

2.1 The following regulatory documents and quality standards were used in developing these Rules:

1) RK ST ISO 9001, Quality Management Systems. Requirements.
2) RK ST ISO/IEC 27001-2023 “Information security, cybersecurity and privacy protection. Information security management systems. Requirements”.’
3) RK ST ISO 9000, Quality Management Systems. Fundamentals and Glossary.

3 Terms, definitions and abbreviations

1) University – Abylkas Saginov Karaganda Technical University NJSC;
2) Management – executive body – the Management Board (Rector’s Office);
3) First Director – Chairman of the Management Board, Rector;
4) Audit criteria – a set of policies, procedures, and requirements;
5) Audit evidence – records, statements of fact, or other information that is related to the audit criteria and can be verified;
6) Audit – a systematic, independent, and documented process of obtaining audit evidence and objectively evaluating it to determine the extent to which agreed-upon audit criteria have been met;

7) Auditor – a University employee appointed by order of the First Director and authorized to conduct an internal audit;

8) Internal audit – an internal audit of the information security management system;

9) QMS – quality management system;

10) ISMS – information security management system;

11) Information Security Service – the University service responsible for information security;

12) Non-conformity – failure to comply with the requirements of an approved regulatory document;

13) Correction – elimination of the identified non-conformity;

14) Corrective action – action taken to eliminate the cause of the identified non-conformity or other potentially undesirable situation;

15) Preventive action – action taken to eliminate the cause of a potential non-conformity or other potentially undesirable situation.

4 Responsibility and authority

4.1 The Information Security Service organizes and coordinates internal audits, develops and updates audit documentation, maintains records, and monitors the implementation of corrective and preventive actions.

4.2 Auditors are responsible for the objectivity, independence, completeness, and reliability of audit results, as well as for maintaining the confidentiality of information.

4.3 Department heads and auditees ensure access to necessary information, participate in the audit, and are responsible for the timely elimination of identified nonconformities.

5 General provisions

5.1 Internal audit is a mandatory element of the University information security management system.

5.2 The purpose of internal audit is to assess the compliance of the Information Security Management System with the requirements of the RK ST ISO/IEC 27001 standard, internal regulatory documents, and the University's actual operating practices.

5.3 Internal audits are conducted on a scheduled and unscheduled basis. The audit results are used by the University management to make management decisions and improve the effectiveness of the Information Security Management System.

5.4 All internal audit records must be documented, stored, and protected in accordance with established requirements.

6 Procedure for conducting internal audit

6.1 Planning of internal audit

6.1.1 Internal audits are conducted by auditors in accordance with the approved annual internal audit plan as set out in Appendix 1 to these Rules.

6.1.2 The annual internal audit plan is developed by the Information Security Service and approved by the University Management no later than December 15 of the current year.

6.1.3 Copies of the approved annual internal audit plan are sent to each employee being audited no later than December 20 of the current year.

6.1.4 Unscheduled internal audits may be conducted using a simplified procedure, without written notice or an Audit Plan but with mandatory documentation of audit findings in accordance with these Rules.

6.2 Training of the Internal Auditor Team

6.2.1 Auditors are selected based on the principle: An auditor should not audit their immediate supervisor.

6.2.2 The Information Security Service is responsible for all stages of the audit.

6.2.3 University Management must promote the development of auditor qualifications.

6.3 Conducting the Audit

6.3.1 The ISS must notify the auditee of the internal audit within 7 working days in any accessible format and familiarize them with the audit program, prepared in accordance with Appendix 2.

6.3.2 The following may be stated as the audit objective:

- Verification of compliance with the requirements of the approved regulatory document;
- Verification of compliance of activities with the requirements of the approved regulatory documents.

6.3.3 The original audit program is kept by the ISS.

6.3.4 Audiees are obliged to inform stakeholders of the upcoming audit.

6.3.5 If the audit cannot be conducted within the time specified in the audit plan, the internal auditor must be notified electronically, stating the reason for the postponement. The internal auditor will then decide on the postponement of the audit. The postponement period shall not exceed one month.

6.3.6 During the internal audit process, auditors collect objective evidence of the compliance of processes with approved regulatory documents through interviews with University employees, examination of documents and observations.

6.3.7 The auditor must record the data obtained during the internal audit in checklists in accordance with Appendix 3 to these Rules. The questions in Column 2 must ensure that reliable and complete information is obtained confirming the presence

or absence of evidence of compliance with the requirements stipulated by the audit program.

6.3.8 Based on the results of the internal audit, the auditor prepares an internal audit report in accordance with Appendix 4 to these Rules and sends a copy to the auditee.

6.3.9 The auditor records each non-conformity report in the Non-Conformity Report Register and transmits it to the auditee.

6.3.10 Within 3 calendar days of receiving the non-conformity report, the auditee develops corrective/preventive actions and sends it to the Information and Security Service. The period for resolving non-conformities is determined by the auditee, but shall not exceed 1 month.

6.3.11 Upon expiration of the nonconformity rectification deadlines, the ISS conducts an unscheduled audit and makes a note in the nonconformity report and in the Nonconformity Report Register.

6.3.12 Audit records must be maintained and stored in the ISS.

6.3.13 The ISS monitors the implementation of the annual internal audit plan, according to its scope of work.

6.3.14 The ISS monitors the implementation of corrective/preventive actions based on the internal audit results.

7 Criteria of the ISMS quality

7.1 The following quality criteria are used in generating the report for management review:

No.	Criterion	Unit	Formula
1.	Compliance with the annual audit plan	%	(conducted planned audits/planned audits)*100
2.	Number of identified nonconformities	pcs	

8 Coordination, approval and implementation

8.1 The list of officials and structural divisions with whom these Rules require approval is determined by the document developer, taking into account the objectives, content, and scope of the ISMS.

8.2 The review period for the draft Rules shall not exceed five business days from the date of its receipt. Comments and suggestions shall be submitted in a reasoned and specific manner.

8.3 If there are no comments, or after they have been taken into account, the document shall be signed by the approving officials and submitted to the executive body, the Management Board, for approval.

8.4 The date of these Rules' entry into force shall be the date of their approval. From the date of their approval, the Rules are binding.

8.5 Upon approval of a new version or amendments, the previous version of the Rules shall cease to be in effect and shall be considered invalid.

9 Safekeeping

9.1 The original of these Rules is stored in the University Information Security Service.

9.2 An electronic version of these Rules is posted on the University corporate information resources, ensuring access for interested structural divisions and authorized employees.

9.3 University employees are familiarized with these Rules in the manner established for the University internal regulatory documents, with the completion of the Familiarization sheet.

9.4 The heads of structural divisions are responsible for maintaining records of copies, preventing unauthorized use, and maintaining the document safety within their respective divisions.

10 Procedure for revising and updating

10.1 These Rules are reviewed by the Information Security Service at least once every two years and are aimed at bringing the provisions of the document into line with current ISMS requirements and changes in the University's processes, structure, and activities.

10.2 Unscheduled updates of the Rules are carried out in the event of changes in the scope of the ISMS, changes in the requirements of the legislation of the Republic of Kazakhstan and information security standards, based on the results of internal audits, analysis of information security inconsistencies and incidents, as well as the implementation of new processes or significant changes to existing ones.

10.3 Amendments and additions to these Rules are issued as a new version or a separate administrative document and are approved in accordance with the procedure established for the approval of these Rules.

Appendix 1
to the Rules of conducting information security internal audits

Approved by
Chairman of the Board, rector of
Abylkas Saginov Karaganda technical University NJSC
_____ S.S. Sagintayeva
Board decision
No ___ dated _____ 2025

Annual plan of internal audit for 20__

No.	Audit purpose	What is audited	Months											Full name of the internal auditor	Note
			January	February	March	April	May	June	July	August	September	October	November	December	
			Dates												
1	2	3	4												5	6

Prepared by: _____ _____ _____
position *(signature)* *(name)*

Appendix 2
to the Rules of conducting information security internal audits

Program
of conducting internal audit

_____
Aditee position (or the audited structural division name)

1. Time and date of the audit beginning _____ _____ 20___
2. Time and date of the audit completing_____ _____ 20___
3. Audit purpose: _____
_____

Audit criteria: _____
_____
_____

4. The audit is conducted in accordance with the requirements

No.	Paragraph of the regulating document	Issues

Internal auditor _____ _____ _____
signature *name* *date*

Person responsible for conducting the audit (auditee) _____
_____ _____
signature *name* *date*

Appendix 3
to the Rules of conducting information security internal audits

Check-list

_____

The auditee position (or the structural division name)

_____ ____, 20__

Paragraphs of RK ST ISO/IEC 27001	**Issue**	**Auditor's observation**

Internal auditor _____ _____ _____

signature *name* *date*

Appendix 4
to the Rules of conducting information security internal audits

Report
On the results of internal audit No. ___

Section 1.
1. Auditee (or structural division):

_____

_____

2. Auditor

_____

3. The audit period from _____ to _____
date *date*

Section 2.
The audit purpose

_____

Section 3.
The audit criteria

_____

_____

Section 4.
The audit results
1. Nonconformity (significant or insignificant):

_____

_____

2. Recommendations on the results of the internal audit:

_____

_____

Auditee _____ _____ _____
signature *name* *date*

Internal auditor _____ _____ _____
signature *name* *date*

F.01-2022

Coordination sheet

Position	Name	Date	Signature
Member of the Board, Vice-rector for Digitalization	Amirov A.Zh.	9.12.25	[signature]
Head of the Legal Service	Ayazbayeva G.S.	9.12.25	[signature]

F.02-2022

Familiarization sheet

Position	Name	Date	Signature