INTERNAL AUDIT RULES
INFORMATION SECURITY

Astana
2023

1. Purpose and scope of application

These Rules for Internal Audit of Information Security of the Information System of the Organization (hereinafter - the Rules) are developed in accordance with the requirements of Sections: 8.2.2 ST RC ISO 9001:2016, 6 ST RC ISO/MEQ 27001:2015.

1. The requirements of these Rules apply to all employees of the Association of RES "Qazaq Green".
2. These Rules regulate the actions of management and employees involved in the internal audit process for information security.
3. Revisions and amendments to these Rules shall be made in accordance with the case law.
4. These Rules shall become effective upon approval.

2. Regulatory References

5. The following regulatory documents and quality forms have been used in the development of these Regulations:

- ST RK ISO 9001-2016 Quality Management System. Requirements.
- ST RK ISO/IEC 27001:2015 Methods and means for securing the information security management system.

3. Terms and abbreviations

Organization - Qazaq Green Association of RES;

IS - information system "Trading Platform for Commodity and Raw Materials Exchanges of Kazakhstan" 2.0;

Audit Criteria - A set of policies, procedures and requirements;

Audit evidence - records, statements of fact, or other information that relates to audit criteria and can be verified;

Audit is a systematic, independent and documented process of obtaining audit evidence and objectively evaluating it to determine the extent to which agreed audit criteria have been met;

Auditor - a staff member of the Organization appointed by order of the First Manager and authorized to conduct internal audit;

Internal audit - internal audit of the information security management system;

QMS - quality management system;

ISMS - information security management system;

Information Security Specialist - an employee of the Organization responsible for information security;

Non-compliance - failure to comply with a requirement of an approved regulatory document;

Correction - elimination of the identified discrepancy;

Corrective action is an action taken to eliminate the cause of a detected nonconformity or other potentially undesirable situation;

Preventive Action - An action taken to eliminate the cause of a potential nonconformity or other potentially undesirable situation;

4. General Provisions

6. The owner of the process is the information security specialist.

7. Internal audits are conducted for the purpose of:

1) verification of compliance of the ISMS with the requirements of ST RK ISO/IEC 27001:2015;

2) Confirmation that an ISMS is being implemented or has been implemented and maintained in the Organization;

3) Demonstrating how close to the rules set out in the ISMS procedures work is performed in the Organization and whether there are differences between the actual work and what is set out in the ISMS documentation.

8. Audits can be of two types:

1) planned audit;

2) unscheduled audit.

9. Audit results are provided to management for the development of corrective and/or preventive actions.

10. Audit records include:

1) annual internal audit plan;

2) internal audit program;

3) check-sheet;

4) report on the results of internal audit.

11. The forms of audit records given in the annexes to this manual are of a recommendatory nature and may be changed depending on the specifics of the Organization's business process.

5. Internal audit procedure

5.1. Internal audit planning

12. Internal audit shall be performed by the auditors in accordance with the approved annual internal audit plan in accordance with **Appendix 1** to these Rules.

13. The annual internal audit plan is developed by the information security specialist, coordinated with the system administrator and approved by the First Head of the Organization, no later than December 15 of the current year.

14. Copies of the approved annual internal audit plan shall be sent to each audited employee no later than December 20 of the current year.

15. Unscheduled internal audits may be conducted according to a simplified procedure, without a written notification and Audit Plan, but with mandatory registration of the audit results in accordance with these Rules.

5.2. Training of the internal audit team

16. Auditors shall be selected based on the principle: The auditor shall not audit his/her immediate superior.

17. The Information Security Specialist is responsible for all phases of the audit.

18. The management of the Organization shall promote the professional development of the auditors.

19. In determining the size and composition of the IS internal audit team, the competence of the audit team is taken into account, based on the level of qualifications of its members.

20. Roles and responsibilities for the internal audit of the Organization are distributed among the members of the audit team. The main groups directly involved in auditing (checking) the knowledge of employees and their compliance with the requirements of normative documents, regulations of the Organization in relation to IS and directly auditing the normative documents defining information security of the Organization are formed.

21. The audit team is provided with workplaces, all necessary regulatory and technical documentation (policies, acts, protocols, contracts, etc.).

22. Appropriate tools shall be used in conducting an internal IS audit. The tools used in IS audits may include tools for automating the analysis of IS compliance.

23. Tools for automating the analysis of IS requirements fulfillment (IS audit criteria) shall allow:

- automate the process of assessing the extent to which IS requirements are met based on their importance;
- Evaluate the effectiveness of different options for protective measures;
- automate the processes of analyzing identified and recorded non-routine user actions and IS incidents;
- generate documented reports with the results of various procedures.

5.3 Instrumental IS auditing.

24. Instrumental audit - identification of software and hardware vulnerabilities by automated inspection methods.

25. The main step in conducting an instrumental audit is to collect all the necessary data about all information assets:

- a list of servers, workstations and communications equipment;
- information about peripheral equipment;
- information on operating systems installed on workstations and servers;
- DBMS data;
- list of application software;
- information on the manufacturer of the protection product;
- configuration settings of the protection tool;
- diagram of the installation of the protection device;
- information on the types of communication channels;
- information about the network protocols used, IP addresses;
- information flow diagram

26. Instrumental security analysis is performed to identify technological vulnerabilities in IS hardware and software.

27. Specialized software tools are used in the tool auditing process. Network scanning is realized in two main stages. At the first stage, initial information about the host was collected, including the list of open ports, information about the type of network services running on the host, etc.

28. The second stage involves searching for vulnerabilities in the network service, which is the main one in the work of the server (for example - web-server).

29. A tool audit also analyzes the configuration settings of system-wide and application software. This audit is aimed at identifying operational vulnerabilities, which include software or hardware configuration errors.

30. At the final stage, a report on the results of the instrumental security audit and general recommendations for eliminating the identified deficiencies in IS assurance processes is generated.

5.4. Conducting an audit

31. The information security specialist shall notify the auditee 7 working days in advance of the internal audit in any available form and familiarize the auditee with the audit program drawn up in accordance with **Annex 2**.

32. The following may be stated as an audit objective:

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

33. The original copy of the audit program is kept with the information security specialist.

34. The auditees, in turn, are obliged to inform the interested parties about the forthcoming audit.

35. In case of impossibility to perform the audit within the time set in the

audit plan, the internal auditor should be notified electronically, indicating the reason for the postponement, who decides on the postponement of the audit. The postponement period shall not exceed one month.

36. In the process of internal audit, auditors collect objective evidence of compliance of processes with approved regulatory documents by interviewing the Organization's employees, reviewing documents and making observations.

37. The data obtained during the internal audit; the auditor shall record in checklists according to **Annex 3** to these Rules. The questions in column 2 shall provide reliable and complete information confirming the presence or absence of evidence of compliance with the requirements stipulated in the audit program.

38. Following the results of the internal audit, the auditor shall prepare a report on the results of the internal audit according to **Appendix 4** to these Rules and send a copy thereof to the auditee.

39. The auditor shall record each nonconformance report in the Nonconformance Report Log and submit it to the auditee.

40. The auditee develops corrective/preventive actions within 3 calendar days after receiving the nonconformance report and sends it to the information security specialist. The period of nonconformities elimination is determined by the auditee, but shall not exceed 1 month.

41. When the deadlines for eliminating nonconformities expire, the information security specialist conducts an unscheduled audit and makes a notation in the nonconformity report and in the Nonconformity Report Registration Log.

42. Audit records must be maintained and kept by the Information Security Officer.

43. Control over the implementation of the annual internal audit plan is carried out by the system administrator and information security specialist, according to their area of activity.

44. Control over the implementation of corrective/preventive actions based on the results of the internal audit is performed by the information security specialist.

6. Responsibility

45. The information security specialist is responsible for organizing internal audits.

46. The Information Security Specialist is responsible for the retention of internal audit records.

47. The Information Security Specialist is responsible for the development and updating of these Rules.

48. Auditors are responsible for non-disclosure of confidential information obtained during internal audits.

49. The System Administrator shall be responsible for verifying that the requirements of these Rules are met.

50. Auditees are responsible for the development and timely implementation of corrective/preventive actions based on the results of internal audits.

51. The auditees shall be liable for failure to fulfill/improper fulfillment of the requirements of the ISMS set forth in these Rules.

7. Quality criteria for an ISMS

52. The following quality criteria are used in generating a report for management review:

№ п	Name of criterion	Univ. amendments.	Formula
1.	Fulfillment of the annual audit plan	%	(planned audits performed/planned audits)*100
2.	Number of identified nonconformities	piece	

Annex 1
to the Rules for Internal Audit of Information Security
"__"_____202_ № _

APPROVED
Director _____
_____
"____"_____202__

Annual internal audit plan for the year 202_.

No. n/a	Purpose of audit	Verifiable	Months of the year												Name and surname of the internal auditor	Notes
			January	February	March	April	May	June	July	August	September	October	November	December		
			Numbers of the month													
1	2	3	4												5	6

SUBJECT: _____ _____ _____
position *(signature) (full name)*

AGREED: System Administrator _____ _____
(signature) (full name).

Annex 2
to the Rules for Internal Audit
information security
"__"_____202_ № _

program
internal audit

_____
Position of the auditee (or name of structural subdivision)

1. Time and date of audit start_____"____"_____**20___year**
2. Time and date of audit completion_____"____"_____**20___year**
3. Audit Objective:

_____

_____

Audit Criteria: _____

_____

_____

4. the audit is conducted in accordance with the requirements

№	Regulatory paragraph	Questions

Internal auditor _____ _____ _____
signature full name date

Responsible for carrying out
audit (audited) _____
signature full name date

Annex 3
to the Rules for Internal Audit
information security
"__"_____202_ № _

Checklist

_____
Position of the auditee (or name. of structural subdivision)
"____"_____**202_**

Items of ST RK ISO/IEC 27001:2015 standards	**Question**	**Auditor's observation**

Internal Auditor _____ _____ _____
signature *full name date*

Annex 4
to the Rules for Internal Audit
information security
"__"_____202_ № _

Report
based on the results of internal audit a No. ___

Section 1.
1. The auditee (or structural unit):

_____

_____

2. auditor:

_____

3. Audit period from_____to _____
date

Section 2.
Audit Objective:

_____

Section 3.
Audit Criteria:

_____

_____

Section 4.
Audit Findings:
1. Non-compliance (significant/insignificant):

_____

_____

2. Recommendations on the results of the internal audit:

_____

_____

Verified _____ _____
signature full name date

Internal Auditor _____ _____ _____
signature full name date

FAMILIARIZATION SHEET

№	Surname, first name, patronymic	Position	Personal signature	Date
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				