18 73

"APPROVED"
Supervisory Board of
JSC "YANGI ANGREN ISSIQLIK
ELEKTR STANSIYASI"
(№ 8/2025 with statement)
Dated 05. 03. 2025 y.

Whistleblowing Policy of JSC "Yangi Angren issiqlik elektr stansiyasi"

1. General Provisions

1.JSC "YANGI ANGREN ISSIQLIK ELEKTR STANSIYASI" (hereinafter – the Company) strives to ensure that its employees comply with the high standards of morality and integrity established in the Company's Code of Ethics. The Code of Ethics requires all employees to conscientiously report actual or potential violations of the Code, as well as any unlawful, illegal, unethical, or dangerous actions.

2.The Company regulates the purpose of whistleblowing, its scope of application, the competent authority to which reports should be submitted, as well as the protection of whistleblowers following bona fide disclosures, through this Whistleblowing Policy (hereinafter – the Policy).

2. Purpose and Scope of the Policy

3. The purpose of the Policy is to establish the obligation of employees to report their concerns and suspected unlawful conduct, as well as to support the Compliance Service and/or the Internal Audit Service in their work.

4. The Company undertakes to protect employees who conscientiously fulfill these obligations from retaliation. The Policy also explains to employees what constitutes protected activity, which reporting channels should be used, and under what exceptional circumstances an employee may disclose relevant information to an authorized external party.

5. The Policy clarifies issues of anonymity and confidentiality, and describes the Company's measures to protect applicants and to prevent any retaliatory actions related to reported unlawful conduct.

6. This Policy applies to all employees of the Company, including members of the Executive Body.

3. Key Concepts and Rules

7. Conduct that violates established standards means non-compliance by an employee of the Company with the Company's Code of Ethics.

8. Protected activity includes reporting information about potential violations of established standards through the channel specified in this Policy. Protected activity also includes assisting a Compliance Service officer and/or an Internal Audit officer in the course of their lawful duties.

9. Retaliation means any direct or indirect harm or adverse action inflicted upon, threatened, or recommended against the applicant as a result of his or her participation in protected activity. Retaliation may include, among other things, discriminatory treatment, changes in salary, demotion, transfer, or dismissal.

10. Applicant — an employee of the Company engaged in protected activity.

11. Employees of the Company must report suspected cases of actual or potential violations of established standards, as well as any actions that damage or may damage the mission and reputation of the Company.

12. In order to be protected under this Policy, the applicant must have reasonable grounds to believe that the information provided is true. Employees who knowingly provide false or misleading information are not considered applicants and, therefore, are not entitled to the protections under this Policy. Submitting false information may constitute a violation and is subject to review by the Compliance Service, and if confirmed, may result in disciplinary measures.

13. The Company encourages employees to report their concerns or suspicions, knowing that they will be protected from retaliation. Identifying the reporting employee may assist the Company in assessing the credibility of the complaint. At the same time, under certain circumstances, the applicant may request that his or her identity remain anonymous or undisclosed.

14. No employee may use his or her position to obstruct other employees from exercising their rights or fulfilling their duties.

4. Implementation of the Policy

15. The applicant must report violations to the Compliance Service; the authorized officer within the Compliance Service is responsible for receiving such reports, providing necessary information and assistance, and ensuring that appropriate measures are taken following receipt of the report.

16. The authorized officer is appointed by the Head of the Compliance Service and works in close cooperation with him. The authorized officer is responsible for ensuring proper awareness within the organization about reporting procedures, receiving any reports and forwarding them to the appropriate officials for review, as well as maintaining contact with the applicant and keeping him or her informed about updates.

17. The applicant may submit a report through one of the following methods:

- via email;
- via postal mail;
- through the hotline;
- by directly contacting the authorized officer.

18. To facilitate proper verification and assessment of the submitted reports, they should, where possible, include the following information:

- a detailed description of the incident that occurred or may occur;
- the place, time, and date of the incident, or when and where it may occur;
- the name and position of the person(s) involved in the incident, or other identifying information;
- the name and position of the reporting employee, if the report is not submitted anonymously;
- the reasons for submitting the report or complaint;
- references to any existing documents confirming the reliability of the reported facts.

19. If the applicant does not wish to report to the Compliance Service using the above methods, he or she may notify the Head of the Human Resources Department, the Head of the Internal Audit Service, or the Director of the Company. Upon receiving the report, the recipient must immediately forward it to the Compliance Service. Reports addressed to any other manager of the Company must also be promptly forwarded to the Compliance Service or to one of the above-mentioned structural divisions of the Company.

20. The Company encourages non-anonymous reports with as much detail as possible. This will help in subsequent actions to determine the validity of the complaint. The applicant may also submit a report anonymously or request that his or her identity not be disclosed. If the identity of the reporting employee is unknown, the authorized officer will make every effort to protect it. Otherwise, the Company cannot provide the protections foreseen by this Policy.

21. The identity of the applicant will be treated with the highest level of confidentiality, except in cases where the applicant has consented to the disclosure of their identity or where otherwise required by law. In such cases, the Company must inform the applicant prior to the disclosure of their identity.

22. The Company recommends that applicants use the internal channels specified in this Policy to report concerns. Internal reporting enables the Company to prevent misconduct or breaches of established rules, as well as to ensure protection against retaliation.
23. In exceptional cases, the Company allows applicants to report potential violations concerning the Company through external channels. Such external reporting is covered by the protections of this Policy if the report is necessary to prevent:

- the emergence of a serious threat to public safety or health;
- significant harm to the Company's activities or violations of national and international law.

24. Any person who decides to submit an external report must strictly comply with the above conditions to be granted protection under this Policy, unless the report is made anonymously.
25. The Company prohibits retaliation against applicants engaged in protected activities. If retaliation by employees is identified, such behavior will be considered misconduct and may result in disciplinary action.
26. Any applicant who believes they have been subjected to retaliation must provide the Compliance Service with all information and documents supporting their claim, using the reporting channels indicated above. The Compliance Service, within its authority, will take measures to prevent retaliation, maintain contact with the applicant, and provide updates regarding the reporting process.

5. Rights of Involved Employees

27. Employees who are or may be the subject of a report must be promptly informed of the allegations made against them, unless such notification would interfere with clarifying the situation.
28. Since reporting of violations and subsequent procedures involve the processing of personal data, such data shall be handled in accordance with applicable legal regulations and the Company's internal documents on personal data protection.
29. The Compliance Service is the department responsible for this Policy. It is responsible for maintaining the relevance of the Policy and incorporating best practices. The authorized officer is responsible for ensuring the effective implementation of the Policy.
30. Each manager, within the scope of their functional responsibility, must comply with this Policy, serve as an example, and provide guidance to their subordinates.

6. Oversight of Compliance with the Whistleblowing Policy Provisions

31. The Compliance Service shall review this Policy at least once every two years or, if necessary, periodically, in order to identify required amendments and additions to achieve the objectives of the Policy, as well as to ensure compliance with applicable laws, internal policies, and Company procedures.
32. Any amendments to the Policy shall be approved by the Supervisory Board upon the recommendation of the Supervisory Board's Anti-Corruption and Ethics Committee.