"APPROVED"

Supervisory Board of

JSC "YANGI ANGREN ISSIQLIK ELEKTR STANSIYASI"

(№3/2025 with statement)

Dated 05. 09. 2025 y.

INFORMATION SECURITY INSTRUCTIONS JSC "YANGI ANGREN ISSIQLIK ELEKTR STANSIYASI"

CONTENT

I. GENERAL PROVISIONS

1. These Instructions have been developed in accordance with the "Regulations on the Information Policy of the Joint Stock Company "YANGI ANGREN ISSIQLIK ELEKTR STANSIYASI" JSC (hereinafter referred to as the Company), as well as the "Regulations on the Organization of the Protection of Confidential Information by Issuers" (No. 2081 dated February 24, 2010) and determines the procedure for referring information to the List of confidential information, as well as the organization of its protection.

2. The following basic concepts are used in this Regulation:

- **confidential information** - documented information, access to which is limited in accordance with the law;

- trade secret - information that has commercial value in scientific, technical, technological, industrial, financial, economic and other areas due to its unknown to third parties, to which there is no free access on a legal basis and the owner of this information takes measures to protect its confidentiality;

- **insider information** - accurate and specific information that has not been disseminated or provided (including information constituting commercial, official, banking secrets, communication secrets (in terms of information on postal money transfers) and other secrets protected by law), distribution or the provision of which may have a significant impact on the prices of financial instruments, goods of the Company.

II. CRITERIA FOR CLASSIFYING INFORMATION AS CONFIDENTIAL

2. The category of confidential information includes commercial secrets, insider information and other information, access to which is restricted.

3. Trade secrets include information that:

has actual or potential commercial value for the Company due to its unknown to third parties;

does not possess signs of state secrets and other secrets protected by law

not be publicly known or publicly available in accordance with the law;

provided with measures to protect its confidentiality.

4. Insider information includes information specified in Appendix No. 1 to this Regulation.

5. Other information of the Company, to which access is restricted, includes the following information:

I. Information about the production activities of the Company, which is a commercial secret of the Company:

a) information about the production capacities of the Company;

b) information about technological processes;

c) information about plans to expand or curtail production;

d) plans for the long-term development of the Company;

e) developments (know-how) of the Company;

f) information on the promotion of new types of products, goods, works and services to the market;

g) tariff policy strategy;

h) personnel policy strategy;

i) other information.

II. Information on the financial and economic activities of the Company:

a) information on business contracts concluded by the Company with suppliers for the purchase of products, goods, performance of work or provision of services;

b) information on business contracts concluded by the Company with consumers for the supply of products, goods, performance of work and provision of services;

c) information on financial transactions of the Company;

d) information about accounting and reporting data;

e) minutes and reports of the Internal Audit Service of the Company;

f) acts of inspections of the financial and economic activities of the Company by state regulatory bodies;

g) other information.

III. Information about the Company as a participant in the securities market:

a) information about the shareholders of the Company (personal data on individuals and details on legal entities that are not publicly available);

b) information on the type and number of shares owned by the shareholders of the Company, with the exception of information subject to mandatory disclosure;

c) information on the type and number of corporate bonds of the Company owned by the owners of securities;

d) decisions of the Company's management bodies prior to their disclosure by the issuer in accordance with the procedure established by law;

e) any information about the activities of the Company as a joint-stock company that is not publicly available;

f) any' information provided to the shareholders of the Company and not publicly available to other persons;

g) registers of shareholders of the Company;

h) registers of holders of corporate bonds of the Company;

i) registration lists of participants in general meetings of shareholders of the Company;

j) minutes of the Counting Commission, voting ballots;

k) orders of the General Director of the Company;

l) minutes of meetings of the Audit Commission of the Company and extracts from the minutes;

m) conclusions and reports of the Company's auditor;

o) lists of affiliated persons of the Company;

o) statement of accrual and payment of dividends to shareholders of the Company;

p) statement of accrual and payment of interest to holders of the Company's corporate bonds;

c) acts of inspections of the Company's activities in the securities market by the authorized state body for the regulation of the securities market;

r) other information.

III. PROCEDURE FOR INCLUDING INFORMATION, COMMERCIAL SECRET, AS WELL AS INFORMATION THAT MAY AFFECT CHANGE IN THE SHARES PRICE INTO THE LIST OF CONFIDENTIAL INFORMATION

4. Information that is a trade secret, as well as the dissemination or provision of which may have a significant impact on the prices of financial instruments, goods of the Company, is included in the List of confidential information (hereinafter referred to as the List) in the manner prescribed by this Regulation.

5. The maintenance of the List is carried out by the sector of the automated control system and digitalization.

6. To make a decision on inclusion in the List of confidential information, the sector of the automated control system and digitalization is presented with:

a document confirming the actual or potential commercial value for its Company due to its being unknown to third parties;

information that this information is not generally known or publicly available in accordance with the law and requires the necessary measures to protect its confidentiality.

7. To review the submitted information and make a decision on the inclusion of this or that information in the List and their exclusion from it, a responsible Commission is created in the Company.

8. The composition of the Commission and the rules of its work are approved by the General Director.

9.5. The Commission, within three days, considers the information and materials attached to it, submitted by the automated control and digitalization system sector in accordance with paragraph 6 of this Regulation, based on the results of which it makes a decision to include the enterprise in the List.

10. The automated control system and digitalization sector continuously monitors the information included in the List.

11. If, based on the results of monitoring, information is identified that does not meet any of the criteria specified in paragraph 3 of this Regulation, the automated control and digitalization system sector, together with the Commission, decides to exclude it from the List.

IV. ADMISSION OF EMPLOYEES OF THE COMPANY AND OTHER PERSONS TO CONFIDENTIAL INFORMATION

12. The following persons have access to the Company's confidential information:

a) a person exercising the functions of the sole executive body (Managing organization, temporary sole executive body), as well as a collegiate body;

b) members of the Supervisory Board and the Internal Audit Commission of the Company who have received access to confidential information in order to fulfill their obligations to manage the Company;

c) persons who own at least 25 percent of voting shares of the Company;

d) persons who have access to the Company's confidential information on the basis of agreements concluded with relevant persons, including auditors (audit organizations), appraisers (legal entities with which appraisers have concluded employment contracts), professional participants in the securities market, credit organizations, insurance organizations;

e) persons assigning ratings to the Company, as well as to the Company's securities;

f) employees who have received access to the Company's confidential information in accordance with their official duties, including employees of the Company's Internal Audit Service;

g) other persons in the cases and in the manner prescribed by law.

13. In order to keep records of persons having access to the Company's confidential information, the List of persons having access to the Company's confidential information should be maintained.

14. The structural subdivision responsible for maintaining the List and exercising control over the circulation of such information is the Department (name of the department).

15. Issuance of archival documents containing confidential information is carried out only on the basis of a list of persons approved by order of the General Director of the Company who has access to archival documents containing confidential information.

16. Admission of persons to confidential information of the Company is provided by the General Director of the Company subject to the following conditions:

a) registration of a written obligation on the preservation and non-disclosure by the employee of information constituting confidential information;

b) familiarization of persons with the requirements of the legislation on ensuring the protection of confidential information.

17. Employees of the Company may receive access to information constituting confidential information of the Company only within the limits of their official duties and to the extent that they really need to perform them.

18. The General Director of the Company is personally responsible for the legitimacy of issuing access to information constituting confidential information to employees.

19. Persons with access to confidential information are required to:

a) strictly keep confidential information classified as confidential information;

b) comply with the requirements of the law to ensure the protection of confidential information;

c) work only with those information and documents containing confidential information to which they have gained access;

d) not use confidential information for personal purposes;

e) immediately inform the General Director of the Company about attempts by unauthorized persons to obtain confidential information from employees, about the loss or shortage of paper and electronic media of confidential information, keys to premises, vaults, safes where documents containing confidential information are located, and about other facts that may lead to the disclosure of confidential information, as well as the reasons and conditions for the leakage of confidential information;

f) in case of termination of relations by a person due to which this person had access to confidential information (layoffs), transfer all paper and electronic media of confidential information that were at his disposal in connection with the performance of his functional duties to the General Director of the Company.

g) employees may also have other duties in accordance with the law.

20. A person is subject to exclusion from the Company's List on the day following the day when the Company learned about the termination of relations with the person, by virtue of which this person had access to confidential information.

21. The General Director of the Company must take the necessary measures to exclude the possibility of getting acquainted with confidential information of employees who do not need it in the performance of their official duties.

V. ORGANIZATION OF THE PROTECTION OF CONFIDENTIAL INFORMATION

22. The Company takes the necessary measures to ensure the protection of confidential information in accordance with the law.

23. Protection of confidential information by the Company is carried out in order to prevent leakage, theft, loss, distortion, blocking, forgery of confidential information and other unauthorized access to it, as well as to prevent unauthorized actions to destroy, block, copy, distort confidential information and other forms of interference in information resources and information systems of the Company.

24. Organization and implementation of control over ensuring the protection of confidential information is assigned to the responsible employee of the Company, appointed by the General Director of the Company (hereinafter referred to as the responsible employee of the Company).

25. The organization of the protection of the Company's confidential information is carried out by complying with the following requirements:

a) compiling and approving a list of the Company's confidential information, familiarizing each employee of the Company with the list of the Company's confidential information and signing an obligation not to disclose confidential information, stipulating in the Company's internal documents, employment contracts and job descriptions of the Company's employees responsibility for disclosure of the Company's confidential information;

b) differentiation of access to confidential information;

c) requirements for the procedure for recording, storing and working with confidential information;

d) requirements for the protection of confidential information in the structural divisions of the Company;

e) requirements for the premises where the technical means processing confidential information are located;

e) requirements for repositories, where the proper storage of documents containing confidential information is ensured;

g) requirements for technical means on which confidential information is stored and processed;

h) requirements for the software of the Company;

i) requirements for control over ensuring the protection of the Company's confidential information;

j) requirements for disclosure of confidential information of the Company.

VI. PROCEDURE FOR RECORDING, STORING AND WORKING FROM CONFIDENTIAL INFORMATION

26. Confidential information of the Company may be contained in documents of the current period and in archival documents.

Confidential information may be contained on paper and electronic media (electronic documents, copies of databases, text, tabular and graphic files containing confidential information).

27. Accounting, storage and work with documents of the current period containing confidential information is carried out in the structural divisions of the Company in accordance with internal regulations.

Accounting for archival documents containing confidential information is kept in the relevant journals in paper and (or) electronic form.

Archival paper documents are stored in the Archive of the Company within the terms established by the legislation.

28. Documents of the Company containing confidential information shall be submitted to the Archive of the Company no later than 3 (three) months after the end of the next financial year.

29. Archival documents containing confidential information must be stored in the premises of the Society's Archive in metal cabinets and (or) safes, which must have strong bolts and be sealed (sealed) outside working hours.

30. It is forbidden to store archival documents containing confidential information in places not intended for storing such documents.

31. Work with archival documents containing confidential information is carried out only in office premises.

32. Sending a document containing confidential information by mail is carried out in the manner prescribed by law.

33. The fact of familiarization with archival documents containing confidential information is subject to registration on the record card of issued archival documents (cases) containing confidential information, and in the register of documents containing confidential information, in the form in accordance with Annexes No. 2 and No. 3 to these Instructions .

34. Reproduction, copying, replication or disclosure of the content of a document containing confidential information is carried out only in cases provided for by law, on the basis of a written permission of the General Director of the Company.

35. Documents containing confidential information selected for destruction, before being handed over for processing as waste paper, must be shredded to an extent that precludes the possibility of reading the text, or must be burned in a specially designated place.

36. After the destruction of documents containing confidential information, a corresponding mark is put in the register.

37. The issuer must take the necessary measures to ensure the protection of confidential information from leakage and unauthorized access when using information and communication technologies (hereinafter referred to as ICT).

38. Access to premises hosting ICTs and databases that process confidential information is restricted to authorized persons.

39. Persons operating and maintaining ICTs are required to:

a) comply with established requirements for ensuring the protection of confidential information when using ICTs;

b) comply with the established regime for restricting access to confidential information;

c) immediately inform their immediate superior or the General Director of the Company about all the facts of attempts of unauthorized access to confidential information, leakage or damage to such information.

40. Connection of ICT to public networks should be carried out only if there is a production need and only with the use of information security tools.

41. In the event of failure or decommissioning of ICTs that processed confidential information, it is necessary to take measures to completely destroy the information contained in them in order to prevent its recovery.

VII. REQUIREMENTS FOR PROTECTION OF CONFIDENTIAL INFORMATION IN STRUCTURAL SUBDIVISIONS OF THE COMPANY

42. When working with confidential information on paper and electronic media in the structural subdivisions of the Company, the employees of the Company must ensure its safety and accounting.

43. The structural subdivisions of the Company that use confidential information in their work are subject to the following requirements:

a) storage of documents containing confidential information in metal cabinets and/or safes specially designated for these purposes;

b) compliance with internal regulations for working with documents containing confidential information;

c) paper documents located on the desktops of the Company's employees should not be available for viewing by unauthorized persons;

d) prevention of leaving documents containing confidential information unattended when leaving the workplace (lunch break, work break, leaving work);

e) when employees leave the premises, paper documents are placed in a lockable desktop box, after the end of the working day they are stored in lockable metal cabinets and / or safes in the premises of the relevant structural unit of the Company;

f) copying and modification of paper documents is carried out strictly in accordance with the internal regulations of the Company, registration and accounting of copying and modification is kept;

g) the destruction of paper documents is carried out strictly in accordance with internal regulations;

h) control by the head of a structural subdivision over compliance by its employees with the requirements established in the Company in relation to access to documents containing confidential information.

VIII. REQUIREMENTS FOR PREMISES WHERE THE TECHNICAL FACILITIES PROCESSING CONFIDENTIAL INFORMATION ARE LOCATED.

44. The Company must compile a list of premises where the technical means processing the Company's confidential information are located (production premises, accounting, legal service, office of the department of corporate relations with shareholders and other structural divisions of the Company).

45. The following requirements apply to the premises where the technical means processing the Company's confidential information are located:

a) installation of lockable metal doors in these premises;

b) equipping the premises with security and fire alarms;

c) observance in these premises of the appropriate mode of operation of technical means processing confidential information (temperature, humidity level and other requirements stipulated by the operating conditions of technical means);

d) restriction of free entry of visitors and unauthorized persons to these premises;

e) the presence of protective measures to prevent unauthorized connection to technical means that process confidential information.

IX. REQUIREMENTS FOR STORAGE WHERE PROPER STORAGE OF DOCUMENTS CONTAINING CONFIDENTIAL INFORMATION IS ENSURED.

46. Documents of the Company containing confidential information must be stored in a storage specially designed for this purpose - in the Archive of the Company, where other archival documents on the activities of the Company are stored.

47. The Archives of the Company must ensure proper storage of documents containing confidential information.

48. The following requirements apply to the Archive of the Society:

a) installation of lockable metal doors in the premises of the Society's Archives;

b) metal bars on the windows;

c) equipping the premises of the Archive with security and fire alarms;

d) observance in these premises of the appropriate regime for storing documents (temperature, humidity level and other requirements stipulated by the conditions for proper storage);

e) equipping the Society's Archive with metal cabinets and/or safes;

f) availability of a separate safe for storing insurance copies of especially valuable documents of the Company;

g) restriction of free entry of visitors and unauthorized persons to the premises of the Archive.

X. REQUIREMENTS FOR SOFTWARE OF THE COMPANY.

49. To ensure information security and protect confidential information, it is necessary to comply with the following requirements for the Company's software (system, network and application):

a) appropriate system software that maintains the operability of the system environment (operating system of servers and workstations, etc.);

b) relevant network software supporting the functionality of the Company's local network;

c) appropriate application software that maintains the functionality of the application software;

d) the availability of relevant documentation for the application software;

e) the ability to differentiate the level of access to users of application software;

e) the ability to back up application databases;

g) proper storage and accounting of applied databases;

h) protection of information from loss, damage, destruction, unauthorized access by unauthorized persons;

i) availability of information recovery procedures.

50. When working with confidential information on electronic media, its protection is ensured by the following measures:

a) prohibition of unauthorized access to information;

b) protection against unauthorized copying, modification and destruction;

c) protection of information from loss and destruction;

d) special and preventive work.

Protection of electronic information from unauthorized access:

a) a password to turn on the computer;

Each workstation (user's computer) must be protected with a password to enable (log in). Employees of the Company must not disclose the password to other persons.

b) differentiation of access to network resources;

Access to network resources is established by the Network Administrator in accordance with the official duties of employees on the basis of a report from the head of the structural unit of the Company.

c) access control to application software functions and databases;

Access to the application software functions and databases is established by the Application Database Administrator in accordance with the official duties of the Company's employees.

d) creation and work with electronic documents only using certified keys;

e) encryption and password protection of individual files with confidential information.

Protection of electronic information from unauthorized copying, modification and destruction:

a) special protection of files for the possibility of copying, modification and destruction;

b) copying and modification of electronic information only in accordance with the Procedure for copying confidential information;

c) destruction of electronic information only in accordance with the Procedure for the destruction of documents containing confidential information.

Protection of electronic information from loss and destruction:

a) operation of servers, workstations, network equipment and other technical means strictly in accordance with the Procedure for the operation of computer facilities and technical equipment;

b) performance of work in electronic databases strictly in accordance with the Instructions for working in application software;

c) the possibility of data recovery in case of emergency shutdowns of programs;

d) anti-virus protection:

Each workstation should be automatically scanned for viruses when the computer is started;

When information is received from e-mail, each workstation should be automatically checked for viruses;

Each workstation should be equipped with anti-virus software to remove detected viruses. Antivirus software must be updated regularly;

The system administrator carries out preventive work on anti-virus protection in accordance with the Information Security Regulations.

Special and preventive work.

a) performance by the System Administrator in accordance with the Information Security Regulations of special works to protect the system environment from changes and preventive work to prevent the destruction of the system environment;

b) performance by the Network Administrator in accordance with the Information Security Regulations of special works to protect the local network from unauthorized access and preventive maintenance to prevent failures in the local network;

c) performance of special works by the Application Database Administrator in accordance with the Information Security Regulations for the protection of electronic databases and preventive work to prevent failures in the operation of the application software.

XI. Requirements for the technical support of the Company.

51. To ensure information security and protect confidential information, it is necessary to comply with the following requirements for the technical support of the Company:

a) the appropriate quality of the technical support of the Company, ensuring its uninterrupted operation under conditions of proper operation throughout the entire period until the resource is depleted;

b) memory capacity sufficient to store information;

c) resource productivity sufficient for information processing;

d) compatibility with other means of technical support used by the Company;

e) operation of servers, workstations, network equipment, uninterruptible power supplies and other technical means strictly in accordance with the Procedure for the operation of computer facilities and technical equipment;

f) maintaining technical equipment in proper working order, timely carrying out preventive and repair work;

g) the use of technical means for hardware protection of confidential information.

XII. Control requirements for the protection of confidential information.

52. The responsible employee of the Company regularly monitors compliance by the Company's employees with the requirements for the protection of confidential information.

53. The responsible employee of the Company is obliged:

a) immediately notify the General Director of the Company about the revealed violation of the requirements of the legislation on ensuring the protection of confidential information (hereinafter referred to as the violation);

b) establish the reasons for the violation;

c) control the elimination of identified violations;

The responsible employee of the Company has the right:

a) make proposals to prevent further identified violations;

b) make proposals on the application of measures of responsibility to violators.

54. When exercising control over ensuring the protection of confidential information, the responsible employee of the Company should pay attention to the following:

a) the correctness of registration data of documents containing confidential information;

b) availability of all documents received and prepared by employees containing confidential information;

c) availability of relevant documents for missing (destroyed, lost, damaged, etc.) documents containing confidential information;

d) compliance with the procedure for storing and working with documents containing confidential information at the workplace, as well as other issues.

55. When violations committed by employees are revealed, the responsible employee of the Company draws up an act on the violation found and submits a report to the General Director of the Company.

XII. Responsibility of persons having access to confidential information.

56. The responsible employee of the Company, who, by order of the General Director of the Company, is entrusted with organizing and exercising control over ensuring the protection of confidential information, is responsible for improper control over compliance by the Company's employees with the requirements for protecting confidential information.

57. The persons specified in clause 19 who have confidential information, including the responsible officer, are not entitled to use this information for personal purposes, as well as transfer it to third parties.

For the disclosure of confidential information, persons having access to such information are liable in accordance with the procedure established by law.

XIII. Disclosure of confidential information.

58. Disclosure of confidential information to third parties is carried out in cases and in the manner prescribed by law.

59. Disclosure of confidential information to third parties is carried out only on the basis of a written request and permission of the General Director of the Company.

60. Requests from third parties for confidential information are recorded in the Company's Confidential Information Register.

XIV. Final provisions.

61. This Instruction comes into force after its approval by the decision of the Supervisory Board of the Company.

62. This Instruction may be amended and / or supplemented in connection with changes in legislation, amendments and / or additions to the Charter of the Company and in other cases.

63. Changes and/or additions to these Instructions come into force after their approval by the decision of the Supervisory Board of the Company.

64. If certain articles of this Instruction conflict with the current legislation of the Republic of Uzbekistan and / or the Charter of the Company, these articles become invalid and in terms of the issues regulated by these articles, one should be guided by the norms of the current legislation of the Republic of Uzbekistan and / or the Charter of the Company until the relevant changes are made to this instruction.