"APPROVED"

General Meeting of Shareholders of the Republican Stock

Exchange "Toshkent" June 20, 2017

Protocol #1

INSTRUCTIONS
on information security
in a joint stock company
RSE "TASHKENT"

Tashkent **2017 г.**

Content

I. General rules

1. This Instruction, in accordance with JSC RSE "TASHKENT" (hereinafter referred to as the Company) "Regulations on information policy", as well as "Regulations on the organization of protection of confidential information by issuers" (No. 2081 dated February 24, 2010) determines the procedure for the development and inclusion of information in the list confidential information, as well as the organization of its protection.

2. This manual uses the following basic concepts:

Confidential information - documented information, the use of which is limited in accordance with the law;

trade secret - information that has commercial value in the field of science and technology, technology, production, finance and economics, as well as in other areas due to anonymity for third parties, which is not legally freely available, the owner of this information takes measures to protect his privacy;

insider information - disclosure or disclosure of the Company's financial instruments that are not disclosed or provided (including trade, services, banking secrecy, communication secrets (in information on the transfer of funds by mail), which may significantly affect the price of its products; other confidential and specific information protected by law.

II. INCLUDING INFORMATION IN CONFIDENTIAL INFORMATION

1. The category of confidential information includes trade secrets, insider information and other information with restricted access.2. A trade secret must have the following characteristics: have real or potential commercial value for its owner due to being unknown to third parties; not have state secrets and other secrets protected by law; not be known or open to the public in accordance with the law; that his privacy is protected.

3. Insider information includes information specified in Appendix 1 to these Instructions.

4. Other Limited Use Company information 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 stop production;

g) long-term plans for the development of society;

d) society's production secrets (know-how);

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

j) tariff policy strategy;

h) personnel policy strategy; T

i) other information.

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

a) Information on business contracts concluded between the Company and suppliers for the purchase of goods, works or services;

b) information on business contracts concluded between the Company and consumers for the supply of goods, works or services;

c) information on financial transactions of the Company;

g) accounting and reporting information;

d) minutes and reports of the internal audit service of the Company;

e) acts of inspection of the financial and economic activities of the Company by state control bodies;

j) other information.

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

a) Information about the shareholders of the Company (personal data of individuals who are not public, and details of legal entities);

b) information on the types and number of shares owned by the shareholders of the

Company, except for information that is subject to disclosure;

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

g) decisions of the management bodies of the company until the moment they are

disclosed by the issuer in accordance with the procedure established by law;

d) any non-public information about the activities of the Company as a joint stock company;

e) any information provided to the shareholders of the Company and not available to

other persons;

j) register of shareholders of the Company;

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

i) a registered list of participants in the general meeting of shareholders of the Company;

k) minutes of the counting commission, ballot papers;

l) Minutes (decision) of the meeting of the Management Board, the Board of

Directors of the Company.

Chairman's orders; - ■

m) minutes of the meeting of the Audit Commission of the Company and extracts from the minutes;

n) conclusions and conclusions of the Company's auditor;

o) List of affiliated persons of the Company;

p) Information on the calculation and payment of dividends to shareholders of the Company;

r) information on accrual and payment of remuneration to holders of corporate bonds of the Company;

c) acts of verification of the Company's activities in the securities market by the authorized state body regulating the securities market;

f) other information.

III INFORMATION, TRADE SECRETIES, ACTIONS

IMPACT ON VALUE CHANGE

DATA AS WELL AS USED

OTHER INFORMATION ABOUT THE LIMITED COMMUNITY

PROCEDURE FOR INCLUDING A SECRET INFORMATION LIST

4. Information constituting a commercial secret, as well as the disclosure or disclosure of which significantly affects the cost 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 instruction.

5. Inventory is carried out by the chief accountant, chief economist, chief of staff and legal adviser.

6. To make a decision on inclusion in the List of confidential information, the Chairman of the Management Board must be presented with:

- a document confirming that the information has real or potential commercial value for the Company due to its anonymity for third parties;

- information that the information is not publicly available or closed to the public in accordance with the law and that its confidentiality is protected.

7. An appropriate commission is created in the Company to review the submitted information and make a decision on its inclusion in the Register or deregistration.

8. The composition of the Commission and the regulations governing its activities are approved by the Chairman of the Board.

9. The Commission, within 3 days, considers the information provided to the head and the materials attached to it in accordance with paragraph 6 of these Instructions and, based on the results, makes a decision to include the information in the Register.

Yu. Rakhbar constantly monitors the information entered in the Register.

11. If, as a result of monitoring, information is found that does not meet the criteria set out in paragraph 3 of these Instructions, the head, together with the Commission, decides to remove it from the register.

IV USE OF CONFIDENTIAL INFORMATION BY PUBLIC AND OTHER PERSONS

12. Confidential information of the Company is used by the following persons:

a) a person acting as an executive body alone (management body, temporary sole

executive body), as well as collectively;

b) members of the Supervisory Board and the Audit Commission of the Company, who have the right to use confidential information to perform the tasks assigned to them for the management of the Company;

c) persons owning at least 25% of voting shares of the Company;

g) Relevant persons, including auditors (audit organizations), appraisers (employment contracts concluded by appraisers with legal entities), professional participants in the securities market, credit institutions, insurance companies acting under an agreement with the Company, have the right to use the confidential information of the Company ;

d) persons rating the Company, as well as the Company's securities;

e) employees who have the right to use the Company's confidential information in accordance with their official duties, including employees of the Company's internal audit service;

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

13. In order to keep records of persons entitled to use the Company's confidential information, it is necessary to organize the maintenance of the List of persons having access to the Company's confidential information.

14. Office department is a structural unit responsible for maintaining records and controlling access to confidential information.

15. The issuance of archival documents reflecting confidential information is carried out only on the basis of a list of persons who have permission to use archival documents reflecting confidential information, approved by order of the Chairman of the Board (decision of the Board).

16. The Chairman of the Management Board of the Company issues permission to the relevant persons to use the confidential information of the Company subject to the following conditions:

a) information constituting the employee's confidential information

a written undertaking to keep and not to disclose

Registration;

b) familiarize the employee with the requirements of the legislation on the protection of confidential information.

17. Employees may have access to information constituting confidential information only within the scope of their official duties and to the extent that they are really necessary for their performance.

18. The Chairman of the Management Board of the Company is personally responsible for the legality of issuing permits to employees to use information constituting confidential information.

19. Persons using confidential information are required to:

a) strict confidentiality of information included in the confidential information;

b) comply with the requirements of the legislation on the protection of confidential information;

c) work with those who have the right to use only information and documents containing confidential information;

d) not use confidential information for personal purposes;

d) attempts by unauthorized persons to obtain confidential information from

employees in paper and electronic form. inform your line manager or the Board of Directors of the Company about the loss or absence of Form n confidential information keys, documents containing confidential information, storage facilities, keys to safes and other facts that may lead to the disclosure of confidential information, as well as the reasons and circumstances to immediately notify chairman;

e) upon termination of relations with a person entitled to access to confidential information (dismissal), he is obliged to provide all confidential information in paper and electronic form that he has at his disposal in connection with the performance of official duties to his immediate supervisor or Chairman of the Management Board. ;

j) An employee may have other responsibilities under the law.

20. The Company removes this person from the Company's List the day after the termination of the relationship with the person who has the right to use confidential information.

21. The Chairman of the Management Board of the Company takes the necessary measures to exclude from this possibility employees who do not need access to confidential information in the performance of their official duties.

V. PROTECTION OF CONFIDENTIAL INFORMATION

ORGANIZATION

22. The Company takes the necessary measures to protect confidential information in accordance with the law.

23. Protection of confidential information by society is the prevention of leakage,

theft, loss, violation, restriction, falsification and other unauthorized use of confidential information, as well as unauthorized actions to destroy, limit, copy, violate confidential information and professional participation in order to prevent other forms of interference into information resources and information systems.

24. The organization and control over the protection of confidential information is assigned to the Company's responsible person (hereinafter - the Company's responsible person), appointed by the Chairman of the Company's Management Board.

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

a) Compilation and systematization of the Company's confidential information, familiarization of each employee of the Company with the list of the Company's confidential information and disclosure of confidential information to them. signing an obligation not to do this, establishing liability for disclosure of the Company's confidential information in the Company's internal documents, labor contracts and job descriptions of the Company's employees;

b) limiting the use of confidential information;

c) requirements for the procedure for accounting, storage and handling of confidential information;

d) Requirements for the protection of confidential information in the structural

divisions of the Company;

d) requirements for premises housing technical equipment for processing confidential information;

e) requirements for storage facilities, which must ensure the proper storage of

documents containing confidential information;

j) requirements for technical means of storage and processing of confidential information;

h) company requirements for software;

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

k) Requirements for disclosure of the Company's confidential information.

VI CONSIDERATION OF CONFIDENTIAL INFORMATION,

STORAGE AND WORK WITH IT

26. Confidential information of the company may be reflected in documents and archival documents of the current period.

Confidential information can be displayed on paper and electronic media (electronic

documents reflecting confidential information, copies of databases, text, tables and graphic files).

27. Accounting, storage and processing of documents reflecting confidential information for the current period is carried out in the structural divisions of the Company in accordance with internal documents.

Records of documents containing confidential information must be kept in appropriate journals in paper and (or) electronic form.

Archival paper documents are kept in the archives of the Company for the period specified in the legal documents.

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

29. Archival documents reflecting confidential information must be stored in metal cabinets and (or) safes in the premises of the Public Archives, which must have a secure lock and be sealed (stamped) during non-working hours.

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

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

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

33. Familiarization with the fact of familiarization with archival documents reflecting confidential information on the registration of the transfer of archival documents (works) reflecting confidential information in registration cards and a journal reflecting confidential information in the form in accordance with Annexes 2 and 3 to this Instruction. resurrected.

34. Reproduction, copying, reproduction or disclosure of the content of a document containing confidential information is carried out only with the written permission of the Chairman of the Management Board of the Company in cases provided for by law.

35. Documents containing confidential information intended for destruction should be disposed of or burned in a specially designated place for this, to the extent that they exclude the possibility of reading the text before it is processed as waste paper.

36. After the destruction of documents reflecting confidential information, an appropriate entry is made in the accounting journal.

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

38. Access to premises where ICTs and databases that process sensitive information are located is restricted to those who have the appropriate access authorization.

39. Persons using and maintaining ICT:

a) comply with the requirements for the protection of confidential information when

using ICT;

b) comply with the established procedure for restricting the use of confidential information;

(c) Immediately notify your line manager or the Chairman of the Board of the

Company of any facts of unauthorized use of confidential information, leakage or leakage of information.

40. The connection of ICT to public systems is carried out only when necessary for production and only with the use of information security tools.

41. In the event of failure or decommissioning of an ICT processing confidential information, measures should be taken to completely destroy the existing information in order to prevent its recovery.

VII. REQUIREMENTS FOR PROTECTION OF CONFIDENTIAL INFORMATION IN THE COMPANY COMPONENTS

42. Employees of the structural divisions of the Company are obliged to ensure its storage and accounting when working with confidential information on paper and electronic media.

43. The Company's subdivisions using confidential information in their work are subject to the following requirements:

a) storage of documents containing confidential information in specially designated metal cabinets and (or) safes;

b) compliance with internal rules for handling documents containing confidential information;

c) paper documents at the workplaces of the Company's employees are closed for public access;

d) do not leave documents containing confidential information unattended when leaving the place of work (lunch, break, dismissal);

d) when an employee leaves the premises, paper documents are placed in a lockable box on the desktop, at the end of the working day - in lockable metal cabinets and (or) safes in the premises of the relevant structural unit of the Company.;

e) copying and modification of paper documents must be carried out in strict accordance with the internal regulations of the Company, copying and modification must be registered and fixed;

j) the destruction of paper documents is carried out in strict accordance with the internal regulations;

h) control over the use by the head of the structural subdivision of documents containing confidential information and compliance with the requirements established by the Company.

VIII. REQUIREMENTS FOR ROOM WITH SECRET INFORMATION EQUIPMENT

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

45. The premises of the Company, where the technical equipment for processing confidential information is located, must comply with the following requirements:

a) installation of lockable metal doors in these premises;

b) provision of premises with security and fire alarm systems;

c) compliance with the relevant operating procedures (temperature, humidity and other requirements established by the requirements for the use of technical means) for the processing of confidential information in these premises;

d) restriction of free access of visitors and outsiders to these premises;

d) availability of security measures to prevent unauthorized access to technical devices that process confidential information.

IX. DOCUMENTS REFLECTING CONFIDENTIAL INFORMATION

EQUIPMENT PROVIDED

REQUIREMENTS FOR STORAGE ROOMS

46. Documents of the Company containing confidential information must be stored in a special room - in the Archive of the Company, where other archival documents related to the activities of the Company are stored.

47. Proper storage of documents containing confidential information in the Company's Archive must be ensured.

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

a) installation of locked metal doors in the premises of the state archive;

b) metal bars on the windows;

c) security of archival premises and fire alarms, provision of tools;

g) compliance with the appropriate procedure for storing documents in these premises (temperature, humidity and other requirements specified in the relevant storage

conditions);

d) provision of the Society's archives with metal lockers and/or safes;

e) availability of a separate safe for storing insured copies of the most important documents of the Company;

j) Limit the free access of visitors and outsiders to the archives of the Society.

X. ABOUT COMMUNITY SOFTWARE

REQUIREMENTS49.

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

a) appropriate system software that supports the operation of the system environment (server operating system, workstations, etc.);

b) relevant network software that supports the operation of the Company's local area network;

c) appropriate application software that supports the operation of the application software;

g) availability of appropriate software documentation;

d) the ability to restrict the use of application software by users;

e) the ability to back up the application database;

j) proper maintenance and record keeping of the practice database;

h) protection of information from leakage, forgery, unauthorized use by unauthorized persons;

i) the existence of information recovery procedures.50. При работе cconfidential

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 distortion

;

d) special and preventive work.

Protection against unauthorized use of electronic information:

a) a password to turn on the computer;

Each workstation (user's computer) must be password protected for activation (access). Society employees

they must not share the password with others.

b) limiting the use of network resources;

The network administrator, on the basis of a notice from the head of the Company's structural subdivision, establishes the use of network resources by employees in

accordance with their job responsibilities.

c) limiting the use of application software and database functions;

The use of application software and database functions is established by the administrator of the application database in accordance with the duties of employees.

g) creation and processing of electronic documents using only certified electronic keys;

d) Encryption and password protection of individual files containing confidential information.

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

a) special protection against copying, modifying and deleting files;

b) copying and changing electronic information only in accordance with the

"Procedure for copying confidential information";

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

Protection of electronic information from loss and damage:

a) the use of servers, workstations, network equipment and other technical means in strict accordance with the "Procedure for the use of computer equipment and technical equipment";

b) perform work in the electronic database in strict accordance with the "Instructions for working with the software";

c) information in case of emergency termination of the program

the possibility of recovery;

g) Antivirus protection:

b) perform work in the electronic database in strict accordance with the "Instructions for working with the software";

c) information in case of emergency termination of the program

the possibility of recovery;

g) Antivirus protection:.

Special and preventive work

a) performance by the system administrator of special work to protect the system environment from changes and preventive work to prevent damage to the system

environment in accordance with the "Information Security Regulation";

b) performance by the system administrator of special work to protect the local network from unauthorized use and preventive work to prevent interruptions in the operation of the local network in accordance with the "Information Security Regulation";

c) Performance of special work to protect the electronic database by the application database administrator in accordance with the "Information Security Regulations" and preventive work to prevent interruptions in the operation of the application software.

XI. TECHNICAL TASTE OF SOCIETY NOTE REQUIREMENTS

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

a) the proper quality of the Company's equipment, ensuring the uninterrupted operation of the Company's equipment throughout the entire period until the development of the resource, subject to proper use,

b) enough memory to store information;

c) the adequacy of available resources for information processing;

d) Compatibility with other service tools used by the Company;

d) strict use of servers, workstations, network equipment, uninterruptible power supplies and other technical means in accordance with the Procedure for the use of computer equipment and technical equipment;

e) timely maintenance, prevention and repair of equipment;

j) the use of technical means of protecting confidential information by hardware.

XII. REQUIREMENTS FOR CONTROL FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

52. The responsible person of the Company regularly monitors compliance with the

requirements for the protection of confidential information by the Company's employees.

53. The responsible person of the company is obliged:

a) immediately notify the Chairman of the Management Board of the Company about

the identified violations of the requirements of the legislation on information security (hereinafter referred to as violations);

b) identify the causes of the violation;

c) monitor the elimination of identified violations.

The responsible person of the company has the following rights:

a) make proposals to prevent identified violations;

b) on the application of sanctions to violators

make suggestions.

54. When monitoring compliance with the requirements for the protection of confidential information, the responsible person of the Company must pay attention to:

a) the correct execution of documents containing confidential information;

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

c) the availability of relevant documents relating to the missing (destroyed, lost,

invalid) confidential information;

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

55. In case of violation of the rules by employees, the responsible employee of the

Company draws up a report on the violation and sends a notification to the Chairman of the Management Board.

XII. USE OF PRIVACY INFORMATION

RESPONSIBILITY OF AUTHORIZERS

56. By order of the Chairman of the Management Board of the Company, the responsible

the person of the Company responsible for organizing and maintaining control over the protection of confidential information is responsible for improper control over compliance with confidentiality requirements by employees of the Company.

57. Persons in possession of confidential information referred to in paragraph 19, including the responsible official, do not have the right to use this information for personal purposes, as well as transfer it to third parties.

Persons licensed to use this information are responsible for the disclosure of confidential information in accordance with the 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 with the permission of the Chairman of the Management Board.

60. Requests from third parties for confidential information must be recorded in the Company's confidential information log.

XIV. FINAL RULES

61. This Instruction comes into force from the moment of approval by the decision of the Supervisory Board of the Company.

62. This Instruction may be amended and / or supplemented in connection with

amendments to the legislation, amendments and / or amendments to the Charter of the Company, as well as in other cases.

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

64. In the event that certain articles of this Instruction conflict with the current legislation of the Republic of Uzbekistan and / or the Charter of the Company, these articles lose their force and, until the relevant changes are made to this Instruction, the issues regulated by this Instruction shall apply to the current legislation. Republic of Uzbekistan.