APPROVED
by Acron Board of Directors
(Minutes No. 615 dd. 21 June 2019)

REGULATION ON INTERNAL CONTROL

to Prevent, Identify, and Restrain Misuse of Inside Information and (or) Market Manipulation

Moscow, 2019

1. GENERAL PROVISIONS

This Regulation on Internal Control to Prevent, Identify, and Restrain Misuse of Inside Information and (or) Market Manipulation ("Regulation") was elaborated pursuant to the provisions of Article 11(2)(1) of Federal Law No. 224-FZ *On Counteracting the Misuse of Inside Information and Market Manipulation and Amending Certain Legislative Instruments of the Russian Federation* dated 27 July 2010 ("Federal Law No. 224-FZ").

This Regulation includes the procedure for accessing inside information, the rules for maintaining its confidentiality, and the rules for monitoring compliance with Federal Law No. 224-FZ.

1.1. Purpose, objectives, and methods for monitoring compliance with Federal Law No. 224-FZ and subordinate regulations

In order to counteract the misuse of inside information and market manipulation, Public Joint Stock Company Acron (also "Company") exercises Internal Control pursuant to the requirements of Federal Law No. 224-FZ and subordinate regulations ("Internal Control").

The key objectives of Internal Control are:

- Detecting risks of regulatory violations by the Company's employees in a timely fashion
- Notifying management (the persons responsible for taking measures to eliminate identified violations) of detected risks
- Making recommendations to eliminate and mitigate detected risks
- Effectively monitoring preventive and restrictive measures and the implementation of recommendations
- Informing (notifying) the Central Bank of Russia of detected suspicious activity/irregular transactions and misuse of inside information in accordance with the procedure adopted by the Company.

Methods and forms of Internal Control:

Monitoring of operations conducted by the Company and its employees (insiders and their related persons).

Control conducted by the responsible officer ("Responsible Officer") commissioned with exercising Internal Control.

Examination of business units' activities (bylaws, job descriptions, audits of database access and time limits for granting and terminating access to inside information).

Regular independent assessment by business units of their compliance with this Regulation.

Instructing and testing employees' knowledge of legal requirements for counteracting the misuse of inside information and market manipulation and their knowledge of internal corporate policy.

Direct monitoring of business units/employees' compliance with legal requirements for counteracting the misuse of inside information and market manipulation.

Communicating to the Company's employees that unfair market practices are unacceptable and providing them with any new regulatory requirements in a timely fashion.

1.2. Procedure for conducting Internal Control for preventing, identifying, and restraining the misuse of inside information and market manipulation

The Company appoints a Responsible Officer, who reports to the sole executive body.

The Company ensures continuous Internal Control.

1.3. Procedure for Continuous Internal Control

If the Responsible Officer is temporarily unavailable, the Company's Chief Executive Officer entrusts the Responsible Officer's functions to another employee.

The Company is the primary employer for the Responsible Officer.

The Responsible Officer may be unavailable for the period of up to one month at a time and for a total of up to two months during a single calendar year, as long as continuous Internal Control is assured. If the Responsible Officer is unavailable for longer than this, the Company's Chief Executive Officer will appoint another person to act as the Responsible Officer.

1.4. Functions, rights and obligations of the Responsible Officer

The Responsible Officer:

- Ensures compliance with this Regulation
- Monitors compliance by the Company and its officers, employees, and clients with the legal requirements for counteracting the misuse of inside information and market manipulation
- Monitors compliance of the Company's business units with the legal requirements for counteracting the misuse of inside information and market manipulation
- Assesses regulatory risk, including risk event probability and its impact on the Company's activity (efficiency of: access measures; protection and safety of inside information; and the procedures and system for preventing, identifying, and restraining market manipulation)
- Where provided for by bylaws, immediately informs the sole executive body or the head of the internal audit service about threatened and committed violations of laws and bylaws concerning Internal Control for preventing, identifying, and restraining the misuse of inside information and market manipulation, and, no later than ten business days after discovery of a violation, delivers a list of measures required to mitigate such risk to officers, including the heads of business units
- Monitors the implementation of measures to mitigate or avoid a regulatory risk
- Takes part in drafting bylaws related to compliance with legal requirements for counteracting the misuse of inside information and market manipulation
- Takes part in drafting bylaws and organising events aimed at compliance with laws on counteracting the misuse of inside information and market manipulation
- Consults employees on applying this Regulation and complying with legal requirements for counteracting the misuse of inside information and market manipulation
- Takes measures to secure the confidentiality of the information they acquire in the course of managing a regulatory risk
- Notifies the sole executive body of any circumstances preventing the Responsible Officer from exercising their functions

When exercising their powers, the Responsible Officer may:

a) Obtain from business units information required to perform their duties, including restricted information

b) Carry out scheduled and unscheduled inspections

c) Independently resolve matters within their scope of authority

1.5. Procedure for exercising the Responsible Officer's duties. Procedure for securing the Responsible Officer's independence

The Company's employees are obliged to immediately inform their line manager or the Responsible Officer about potential and existing violations of laws, constituent documents, and bylaws related to compliance with laws on Internal Control for preventing, identifying, and restraining the misuse of inside information and market manipulation.

The Company's business units and officers must fully carry out the Responsible Officer's requirements related to the performance of the Responsible Officer's duties.

The Company must ensure that the Responsible Officer's objectives are achieved without interference by business units and employees directly involved in an entity's activity (operations, financials, etc.).

The Responsible Officer will not be entrusted with duties that may result in a conflict of interest with their control functions.

The Responsible Officer's activity is independent from other business units.

On behalf of the Company, the Chief Executive Officer will provide the Responsible Officer with:

- Necessary and sufficient resources to achieve the Responsible Officer's objectives
- Access to the information required to perform a relevant function

1.6. Procedure for Revising and Amending This Regulation

In order to improve Internal Control practices, the Responsible Officer may, as needed, submit to the Chief Executive Officer draft amendments and addenda to this Regulation containing the reasons for amending this Regulation.

1.7. Procedure and timeline for retaining documents related to Internal Control for preventing, identifying, and restraining the misuse of inside information and market manipulation

The Company shall ensure that documents related to Internal Control for preventing, identifying, and restraining the misuse of inside information and market manipulation be kept no less than five (5) years from their execution, approval (signing), and review.

2. MEASURES PREVENTING MISUSE OF INSIDE INFORMATION AND MARKET MANIPULATION

2.1. Procedure for accessing inside information, the rules for maintaining its confidentiality, and the rules for monitoring compliance with the requirements of Federal Law No. 224-FZ and subordinate regulations

2.1.1. Subject to Federal Law No. 224-FZ, Company insiders include:

2.1.1.1. Members of the Board of Directors
2.1.1.2. Sole executive body of the Company
2.1.1.3. Members of the collegial executive body (the Managing Board)
2.1.1.4. Members of the internal audit team
2.1.1.5. Contractors with access to the Company's inside information, including: ● external auditors (audit companies), ● appraisers (legal entities with which appraisers have labour contracts), ● professional securities market participants, ● credit institutions, ● insurance companies
2.1.1.6. Information agencies disclosing or presenting the Company's information
2.1.1.7. Rating agencies assigning ratings to the Company and its securities
2.1.1.8. Individuals having access to the Company's inside information under labour and civil law contracts

2.1.1.9. Persons having access to information about the preparation and/or submission of a voluntary, mandatory, or competitive offer to acquire the Company's securities, a notification of the right to demand securities repurchase, or a securities repurchase demand pursuant to Chapter XI.1 of Federal Law No. 208-FZ of 26 December 1995 *On Joint Stock Companies*, including persons who deliver to the joint stock company a voluntary, mandatory, or competitive offer, a notification of the right to demand securities repurchase, or a securities repurchase demand, a bank or another credit institution providing a bank guarantee, and appraisers (as well as legal entities with which such appraisers have labour contracts)
2.1.1.10. Other persons having access to the Company's inside information by virtue of law or contract

2.1.2. The Company shall keep a list of its insiders based on categories of persons specified in Clause 2.1.1. of this Regulation.

2.1.3. Only the persons specified in Clause 2.1.1 of this Regulation may access the inside information, in accordance with their status (authorities and job descriptions, and provisions of a contract, etc.). When entering into an agreement with a legal entity obtaining access to the inside information by virtue of such agreement, such entity shall be informed about requirements of Federal Law No. 224-FZ and subordinate regulations of the Central Bank of Russia, and liability for misuse of inside information, and also that it will be put on the list of insiders. Inside information may be transferred to legal entities pursuant to executed agreements after such entities are on the list of insiders.

2.1.4. Such persons must maintain the confidentiality of all inside information of which they become aware.

2.1.5. The Company provides all necessary administrative and technical conditions to enable persons with access to inside information to maintain the established confidentiality regime.

2.1.6. Persons having access to inside information must:

- Undertake comprehensive measures to keep inside information secure
- Not provide or distribute inside information, except as provided for by current Russian laws
- Upon loss of status as a person with access to inside information, deliver to the Company any physical media in their possession containing inside information
- Company employees with access to inside information are required to promptly inform their line manager, their line manager's deputy, or the Responsible Officer of any lost or missing documents or files containing inside information, safe (storage) keys, passes or passwords. They must also inform their line manager, their line manager's deputy, or the Responsible Officer if they detect unauthorised access to inside information

2.1.7. Any person whose status does not permit access to inside information and who gains access to it must:

- Stop reviewing it
- Take exhaustive measures to the maintain confidentiality of such inside information
- Prevent the inside information from being distributed to or provided to third parties

2.1.8. The Company only responds to third-party requests for inside information when it is required to do so by current Russian laws.

2.2.1. No person may use Inside Information:

- To perform transactions with the Company's securities that are covered by the inside information, whether for themselves or for a third party, except transactions to discharge a

mature obligation to buy or sell the Company's securities arising from a transaction executed before the person learned the inside information
- To transfer the Inside Information to another person, except when transferring it to persons on the list of insiders in order to discharge obligations set forth by federal laws or to perform employment or contractual duties
- To make recommendations to third parties, obligating or otherwise inducing them to buy or sell the Company's securities

2.3.1. In order to ensure (preserve) the confidentiality of inside information, the Company takes the following protection measures:

- Approving the list of information classified as inside information
- Keeping a record of persons having access to inside information and persons to whom such information is provided or transferred
- Regulating the use of inside information by employees through labour contracts and by contractors through civil law contracts
- Establishing access control in buildings and facilities occupied by the Company (on both business and non-business days)
- Ensuring the destruction of all documents and other media that are not subject to retention and may contain inside information
- Introducing technical measures to protect workplaces and places where documents and other media containing inside information are stored from unauthorised access and viewing
- Applying technical measures to protect the Company's IT systems containing inside information from unauthorised access, including through telecommunications channels
- Restricting employees' access to local network resources, establishing an authorisation system for operating floppy magnetic data discs or compact discs, electronic mail, and the Internet, and maintaining encryption for information sent to outside networks
- Taking other measures that do not contradict Russian laws and that are designed to prevent unauthorised access to inside information and to stop its misuse.

2.4.1. The compliance control system for legal requirements to counteract the misuse of inside information includes the following measures:

- Discovering inside information
- Verifying rightful access to inside information
- Monitoring the list of insiders
- Administering the Company's management activity related to compliance with legal requirements for countering the misuse of inside information
- Administering data flow management (data receipt and transfer) and information security
- Uninterrupted monitoring of the inside information control system in order to evaluate its adequacy for the Company's objectives, identify shortcomings, elaborate proposals, and exercise control over implementation of solutions to improve the inside information control system
- Identifying and monitoring in a timely fashion all areas of potential use of inside information, potential conflicts of interest, systematic verification of proper job performance by persons having access to inside information and other employees in order to prevent the concealment of illegal actions
- Uninterrupted monitoring of the inside information control system, with the Company taking necessary measures to improve the inside information control system and ensure its efficient operation, including in response to changes in internal and external factors affecting the Company's activity.