

CODE OF CONDUCT



MOSCOW, 2021



CONTENTS

I.	Purpose and scope	3
II.	Principles of conduct in financial markets	4
III.	Confidential information protection	5
IV.	Receiving and providing information	6
V.	Bad practices	8
VI.	Membership in corporate bodies and committees of Infrastructure Organisations	10
VII.	Using hardware and software	11
VIII.	Final clauses	14



I PURPOSE AND SCOPE

The Code of Conduct (hereinafter referred to as the Code) has been drafted by a joint initiative of the Bank of Russia, financial market self-regulatory organisations (hereinafter referred to as SROs), MOEX Group companies (hereinafter referred to as the Infrastructure Companies), and trading members and (or) clearing members which MOEX Group companies provide their services to (hereinafter referred to as the Organisations). The Code sets out basic principles and rules of conduct the Organisations are advised to follow when dealing with each other, their customers, and others.

The purpose of the Code is to develop and maintain good practice standards which, first and foremost, promote a favourable investment environment in the Russian financial market.

The Code is advisory in nature. However, taking into account a major purpose of the Code, the MOEX Group encourages the Organisations to join the Code¹ and strives to apply the Code's principles in its operations.

The Code also promotes the MOEX Group's mission, namely, to bring trust, efficiency and innovation to financial markets and help the Organisations and citizens in achieving tomorrow's goals.

To promote a culture of trust and responsibility in the Russian financial market, the Organisations are encouraged to inform their customers, customer intermediaries, and counterparties important to sustainability in the Russian financial market (such as specially configured software providers) of the principles of conduct set out in the Code.

The Code is based on generally accepted rules of professional ethics, national and global best practices, as well as on expert opinions of the Organisations. The principles set out in the Code align with approaches proposed by the Bank of Russia, those including with regard to ensuring fair and good conduct in financial markets.

1. The Organisations have the right to declare their adherence to the Code. Information on how to join and who has joined the Code shall be available on the Moscow Exchange's official website.

The Organisations and Infrastructure Companies shall be guided by the interests and needs of the Russian financial market, and shall adhere to the following principles when engaging with each other, their customers and others:

- **Honesty** – financial service providers are sincere in their intentions and actions, respect agreements and values, admit their mistakes and are open to discuss them.
- **Fairness** – financial service providers treat their customers and other stakeholders equally and in a fair way, they do not abuse the opportunities and rights, respect the legitimate interests of the persons concerned, and strive to ensure the product price is appropriate to its value to the customer.
- **Transparency** – financial service providers disclose all necessary information that allows monitoring of their activities in the financial market, and communicate all relevant information to their customers and other stakeholders in a timely manner and to the fullest extent.
- **Customer care** – financial service providers build respectful relations with their customers, give due consideration to their interests, help in dealing with conflicts of interests and in overcoming barriers that prevent persons with disabilities from accessing financial services on equal terms.
- **Protection** – financial service providers build appropriate systems to ensure that customers and their assets are protected from the risks of loss (theft) and other external and internal threats, and ensure security of information protected by law.
- **Professionalism** – financial service providers have appropriate experience, knowledge and skills required to perform their duties, and are committed to upholding the best professional standards.
- **Accountability** – financial service providers understand that they are responsible for the consequences of all actions they take, develop effective mechanisms to separate and enforce responsibilities, as well as risk management and control systems mechanisms.
- **Integrity** – financial service providers strive to support market mechanisms and to raise overall confidence in the financial market and market participants, to declare a common goal for achieving market integrity, to take practical steps to reach that goal, and to promote a culture of integrity.

For the purpose of promoting the principles of conduct, the Organisations and Infrastructure Companies shall strive to comply with the rules of conduct defined in Sections III to VII of this Code when they operate in the financial market.

Knowing that information is a key value for financial markets, the Organisations and Infrastructure Companies give considerable attention to ensuring security of both information expressly protected by the applicable law (including personal data, insider information, commercial and banking secrets) and any other information which, if disclosed, may cause harm to the Infrastructure Companies, Organisations or their customers (all information listed in this paragraph is hereinafter referred to as confidential information).

When developing confidential information protection mechanisms, while supporting the principles of **professionalism, accountability, protection and integrity**, the Organisations and Infrastructure Companies have agreed to adhere to the following rules of conduct:

A. Ensure that staff members, whatever their jobs are, treat all information they deal with responsibly and attentively, also through the following:

- continuous development of their professional competence with regard to confidential information protection;
- incentives to employees who detect and report, in good faith, vulnerabilities they identify in the system protecting confidential information from unauthorised access;
- zero-tolerance approach to employees' negligence in protecting confidential information.

B. Ensure adequate and modern-day technical infrastructure to protect confidential information from unauthorised access.

C. Promptly respond to any confidential information leakage threat or incident, and continuously improve confidential information protection systems.

D. Avoid conflicts between confidential information protection and transparency and availability of non-confidential information, including a commitment to procedures relating to disclosure of information material to all financial market participants.

E. Make confidential information available on requests from public, judicial or supervisory authorities only if these meet requirements of the applicable law.

IV RECEIVING AND PROVIDING INFORMATION

The Organisations fully understand that following the principles of conduct, such as honesty, transparency, protection and integrity towards non-confidential information helps to keep relevant the information that is material for financial market entities and to minimise risks arising from untimely access to data about events that may affect stability of the financial market system and its members.

Given that providing insufficient or unreliable information to financial market entities, these including the Infrastructure Companies, may potentially adversely affect the Organisations and their customers, the Organisations have agreed to adhere to the following rules of conduct:

A. The Organisations do their best to ensure that the Infrastructure Companies are informed in as full, detailed and timely a manner as possible of the following (including but not limited to):

- data on the Organisation and its customers to the extent necessary for admission to organised trading, clearing and registration and to assess the risk level for the Organisation;
- facts that need to be considered while determining transactions and operations acceptable to the Organisation and/or its customers, with due consideration given to restrictions that may be imposed by state authorities/the Bank of Russia/issuers/other financial market entities.

B. In engaging with their customers, the Organisations do their best to provide the fullest and most detailed information necessary for their customers to make decisions on organised trades on behalf of the Organisations, in particular, on the following:

- procedures to execute and settle transactions on organised trading, a need to give assets as collateral for such transactions, and default management instruments applied by the Infrastructure Companies;
- requirements of the Infrastructure Companies to provide them information on such customers to enable transactions on behalf of customers and settlement of obligations under such transactions;
- failures and/or faults of software and/or hardware of Organisations, their providers and communications service providers, Infrastructure Companies when these may negatively affect customer operations, as well as measures that the customer needs to take in response to such failures and/or faults, and the time and procedure for system recovery, including the resumption of organised trading/clearing;

- possibility, terms and conditions of segregation² and portability³ provided by the Infrastructure Companies and advantages of using it;
- existing and new products and services offered by the Infrastructure Companies, also based on investment objectives of such customers when they operate in the financial market, as well as on the risks inherent in the relevant products and services;
- financial market events with customers (conferences, forums, seminars, contests, etc.) focused on presenting new and existing products and services to promote a more attractive financial market, raise financial literacy and investor interest in the Russian financial market.

C. The Organisations fully understand that market data generated by the Infrastructure Companies is essentially derived by calculating and aggregating, with the use of particular methodologies and principles, the entire or part of the data provided by each Organisation in the course of its activities in the financial market. Therefore, for avoiding infringement of legitimate interests of the owners of both output information (market data) and underlying information (including that available in transaction orders), the Organisations have agreed on the following key rules of conduct:

- The Organisations regularly verify compliance of their employees, customers, investors and others with market data use requirements.
- The Organisations regularly inform their customers and investors on the methods for obtaining market data and its possible use, applicable limitations, as well as on information audits (when trading on organised markets for the benefit of customers).

D. Being aware of potential risks, including those of a systemic nature, that may arise from bad conduct of one or more financial market entities, the Organisations do their best to prevent and address them. In particular, the Organisations are encouraged to communicate to the Infrastructure Companies the following information:

- information on non-performance/undue performance by issuers of their obligations, including, but not limited to, obligations to pay income on securities, to carry out mandatory corporate actions, to ensure that the Infrastructure Companies take the necessary measures to avoid negative consequences of unfair behaviour and to prevent such situations from recurring in the future;

2. A mechanism set out in the laws and clearing rules for separate accounting of customer's assets held as collateral against obligations in the central counterparty's internal accounting system.

3. A mechanism set out in the laws and clearing rules that allows a separate customer to initiate transfers of its positions and collateral from one clearing member to another, also in case of default of the initial clearing member.

- information on a conflict situation arising from execution of transactions, so to ensure that the Infrastructure Companies take measures to further resolve such conflict situation, in particular by identifying ultimate counterparties and ensuring their interaction with the Organisation;

E. When a conflict situation arises, the Organisations take every possible effort to resolve it through negotiations, in an honest, mutually respectful and trusting manner, without bias, unfair criticism, and baseless written and/or verbal requests, statements, complaints that may discredit others.

V **BAD PRACTICES**

While following the principles of **fairness, customer care, protection, accountability** and **integrity**, the Organisations seek to ensure fair pricing for financial instruments, foreign currency and (or) commodities, equal opportunities for investors and investors' stronger confidence in financial markets.

Creating and maintaining an effective risk control and management system that helps to identify and adequately assess existing and potential risks in the Organisation's operations is a key stepping stone towards this goal.

The Organisations take every effort available and necessary to prevent, identify and suppress bad practices in the financial market, in particular, through monitoring and reviewing transactions and operations. However, the scope of such monitoring and verification process shall not be limited to customer transactions and operations, but shall also focus on preventing, identification and suppression of bad practices in Organisations' transactions and operations.

The Organisations' monitoring and verification system shall identify bad practices in organised trading (if applicable) recognised as such in accordance with the Russian law, including those relating to:

- creation of false or misleading bids/asks for financial instruments, foreign currency and (or) commodities using HFT algorithms;

- creation of false or misleading bids/asks for financial instruments, with a change in their price due to the market maker's unfair performance;
- changes in prices of financial instruments, foreign currency and (or) goods by prior agreement between trading members and (or) their employees and (or) their customers, including via information and telecommunication networks to which access is not restricted to a certain number of persons;
- execution of transactions at prices that deviate materially, solely to secure a positive outcome for one counterparty against the other counterparty's loss;

To prevent, detect and suppress such practices, the Organisations may apply, inter alia, SRO recommendations.

The monitoring and verification system is not limited to detecting the above-mentioned cases. The system is also verified to ensure that it covers controls reasonably necessary to manage all the risks which are responsibility of the internal control (compliance) service of the Organisation concerned (such as risks of ML/FT&WMD proliferation, conflict of interests, corruption and licensing violation risks).

For the stable development of the Russian financial market, the Organisations take reasonable efforts to create a culture of conduct and to suppress bad practices in financial markets that go beyond the minimum legal requirements, in particular:

- introduce the principles of conduct in financial markets set out in the Code to their employees involved in financial market transactions on behalf of customers or their own behalf, and explain why it is important to follow the relevant principles when making professional decisions;
- highlight the principles of conduct in financial markets, common bad conduct scenarios at organised trading, accountability for such bad conduct (practice) in information materials/trainings customers;
- help the Infrastructure Companies in organising control over transactions at organised trading, particularly to prevent, identify and suppress unauthorised use of insider information and (or) market manipulation, by providing the necessary documents (including those received by the Organisation from its customers), explanations and information to the Infrastructure Companies upon their request.

Development of diverse activities in the financial market, assurance of effective financial market mechanisms and institutions that exist, as well as creation of new ones will be only possible through active and effective engagement of all financial market entities in the decision-making process that concerns each category of financial market participants, their customers, as well as the Infrastructure Companies.

The Organisations have the opportunity to influence further developments and address the interests and opinions of all parties involved in financial market relations, also in relation to organised trading activities, through the functioning advisory bodies and user committees of the Infrastructure Companies. The Organisations fully understand how important the role of user committees and advisory bodies is, and how much influence collegiate decisions taken have, therefore the Organisations adhere to the principles of professionalism and accountability and treat their membership in such committees and advisory bodies in the most responsible and disciplined manner possible. In particular:

A. They ensure that their authorised representatives having necessary expertise and knowledge of the issues under consideration attend the meetings of user committees and/or advisory bodies of the Infrastructure Companies. The authorised representatives are encouraged to take a proactive role in the professional community, also through their membership in professional associations that discuss innovations and open issues and develop best financial market practices.

B. Through their membership in user committees and/or advisory bodies of the Infrastructure Companies the Organisations ensure:

- balancing the interests of the Russian financial market, professional community with the interests of the Organisations while developing proposals, participating pro-actively in discussions and making decisions.
- taking responsible attitude to their work in user committees and/or advisory bodies of the Infrastructure Companies, also avoiding unnecessary absence from meetings.
- responsible use of information they receive through their membership in user committees and/or advisory bodies of information, taking into account possible consequences of information dissemination or disclosure to the third parties.

- keeping the concerned units and officials of the Organisations well and fully informed of positions/decisions developed/reached during the membership in such user committees and/or advisory bodies, so that the Organisations take timely actions to improve their internal procedures or technologies.

C. They are aware that opinions and decisions delivered by their representatives during the meetings or voting at the meetings of user committees and/or advisory bodies are regarded by others as opinions and decisions of the Organisations.

VII USING HARDWARE AND SOFTWARE

Raising the level of stability and effectiveness of the Russian financial market largely depends on whether the Organisations and Infrastructure Companies ensure a strong operational reliability while developing their business processes and services technologically.

For effective and stable operations, as well as to ensure that the Organisations, Infrastructure Companies and their customers use any hardware and software, including trading and clearing systems, in good faith while operating in financial markets, the Organisations set out the following rules of conduct promoting the principles of honesty, accountability, protection and integrity:

A. They use only licensed software, uninterrupted power supply tools, antivirus tools, fail-safe communication channels and data copying systems.

B. They have and apply appropriate tools to protect data (including personal data) from loss, corruption or accidental destruction, and to recover data after computer failures.

C. They analyse software in terms of its potential use in violation of applicable laws and minimisation of risk of such misuse.

D. On a regular basis the Organisations:

- upgrade and test their hardware/software for fault tolerance and operational safety, and actively participate in testing of trading and clearing system upgrades;
- test software and/or hardware they and their customers use, and immediately response to faults and failures if any occur.

E. They comply with requirements and recommendations from the software developers and Infrastructure Companies regarding the use of software and hardware, in particular, regarding a maximum load and measures to control that their customers use software and/or hardware in a proper way.

F. The Organisations make every effort available to prevent, identify and minimise negative consequences of:

- operational risk events involving their software and/or hardware, also in cases where the Organisations have engaged third party suppliers to provide technical services to them or to their customers needed for them to perform their exchange market activities (hereinafter, the third-party suppliers), as well as possible negative effects of these events on other Organisations, also through the Infrastructure Companies;
- unauthorised access to software and (or) hardware of the Organisations, also those involving the software and/or hardware of the Infrastructural Organisations, and of unauthorised access to software and/or hardware of the Infrastructural Organisations.

G. The Organisations notify:

- their customers on risks relating to the use of software and/or hardware, methods to minimise/response to such risks, and on requirements to report any case/attempt of unauthorised access to software and/or hardware;
- Infrastructure Companies on any attempt/case of unauthorised access to software and (or) hardware of the Organisations and/or their customers, involving software and/or hardware of the Infrastructural Organisations, and of unauthorised access to software and/or hardware of the Infrastructure Companies. The Organisations provide the Infrastructure Companies with information relating to unauthorised access attempts/cases, findings of their investigations and assist in any other way;

- Infrastructure Companies on abnormal and emergency situations, these including system-wide and process failures in software and/or hardware of Organisations, their customers or third-party suppliers, which they think create risks of interruption of software and/or hardware of other Organisations or Infrastructure Companies, as well as when circumstances creating such situations stop to exist.

H. They ensure continuous operation of their communication systems, including those to connect to the Infrastructure Companies, and have available emergency connection methods if software and/or hardware of the Organisations or Infrastructure Companies fails.

I. They comply with requirements for transferring software and/or hardware received from the Infrastructure Companies to their customers, in particular, mandatory registration of such customers and properly obtained consent from the Infrastructure Companies.

To avoid operational risks, disruption in operations of any software and/or hardware, inclusive of trading and clearing systems, used by the Organisations or their customers in their financial market activities, including through the Infrastructure Companies, and to maintain continuous and secure activities, the Organisations acknowledge it unacceptable that the Organisations or their customers:

A. use software and/or hardware, introduce new services or any updates (modifications), if it creates or may create a threat to normal operation of software and/or hardware of other Organisations, also through the Infrastructure Companies, violates and/or interferes with the rights of other Organisations and Infrastructure Companies;

B. use automated systems to submit HFT orders, if it creates or may create a threat to the normal operation of other Organisations' software and/or hardware, also through the Infrastructure Companies;

C. use software and/or hardware conflicting with software and/or hardware of the Infrastructure Companies.

VIII FINAL CLAUSES

The Organisations understand that it is important to follow the principles of conduct in all aspects of their activities, including in cases not covered by this Code.

The Organisations declare their commitment to the conduct standards by signing the declaration form (see Annex 1) and notifying MOEX thereof.

If MOEX identifies that the Organisations do not comply with the principles set out in this Code, MOEX may exclude such Organisations from the list of those having joined the Code published on its website.

If a violation of the Code or a situation related to the Code or its scope is identified, the appropriate information can be submitted in the manner described on the MOEX's website. If necessary, the Bank of Russia, SROs and Organisations may be invited to deal with complaints relating to the Code (in particulate, within a working group format). The outcomes from dealing with complaints may be published on the website of MOEX. Complaints are dealt with and information is published in an anonymised form (without mentioning the name(s) of the contacted person(s) or the person(s) affected by the recorded violation(s).

The Organisations will seek to identify changes/challenges/areas of development in the Russian financial market that affect other Organisations, customers and Infrastructure Companies, and to develop their proposals on the necessary rules of conduct that need to be followed to achieve the common goals of the Russian financial market. The Organisations have agreed to amend this Code as and when necessary.

**SIGN-UP (DECLARATION) FORM
FOR JOINING THE CODE OF CONDUCT**

We [organisation name] (hereinafter, the Organisation) hereby declare our adherence to the Code of Conduct developed by a joint effort of the Bank of Russia, SROs in the financial market, MOEX Group companies, and the Organisations that are trading and/or clearing members using the services of MOEX Group companies, as posted on the official website of MOEX (hereinafter, the Code).

We have reviewed the Code and acknowledge that the Code provides a set of global principles recognised as good practice in financial markets. We also affirm our commitment to the principles set out in this Code.

I hereby confirm that I have the authority to sign this sign-up form (declaration) for joining the Code of Conduct.

[job title name]

[organisation name]

[date]

_____ [full name]

[signature, seal]