APPROVED
Order No. МБ-П-2023-1597
Dated 20 June 2023

RULES FOR PROVIDING TECHNICAL ACCESS TO MOSCOW EXCHANGE SOFTWARE AND HARDWARE COMPLEX FOR USERS

1. Overview

1.1 The procedure for giving Technical Access to Users is set out in accordance with the Terms of Integrated IT Service available on the Technical Center's website at http://moex.com/a1819, internal documents of the Technical Center and these Rules constituting an integral part of the Terms of Integrated IT Service.

1.2 Terms used in these Rules have the meanings ascribed to them in Russian laws and regulatory acts, the Moscow Exchange's Charter, trading rules and admission rules, admission regulation for MOEX's Money Market and other regulations of Moscow Exchange, clearing rules and other regulations of the Clearing Center as well as regulations of the Technical Center.

1.3 These Rules may be amended or supplemented. The Rules as amended from time to time are available at http://moex.com/a1819.

1.4 To bring the process of operation of the User's hardware and software used for Technical Access to the TC SHC under control, the User must appoint an employee (the "Service Administrator") who will be responsible for:

- Technical maintenance and the hardware and software safety;
- Ensuring restricted access to the hardware and software;
- Timely instant communication with the Technical Center's technical support service.

1.5 The User must indicate relevant and reliable information about the Service Administrator in the Legal Entity Questionnaire submitted under the Information and Reporting Provision Rules available at https://fs.moex.com/files/7500.

1.6 The requirements and technical specification set out in these Rules are also applicable if the User assigns the right to use the software under the Integrated IT Service Terms to its Clients. In this case, the User shall be responsible for ensuring that the Clients meet the requirements set out in these Rules while connecting the software to the Technical Center's SHC under the Integrated IT Service Terms.

2. Technical specifications for Technical Access via Remote Workstation

2.1 To get Technical Access to the TC SHC Subsystems by using Remote Workstations provided under the Agreement, the User should contact the Technical Center and then take actions to acquire and install a Remote Workstation by following instructions received from the Technical Center. It is the User's responsibility to install, put into operation and maintain a Remote Workstation, or hire at its own expense specialized companies (a specialized firm (including the Technical Center) to do those things with the assistance of, and under control of the Technical Center.

2.2 The connectivity scheme used on Remote Workstations must comply with one of MOEX's prescribed schemes for access to the TC SHC which are available at https://www.moex.com/s653.

2.3 If operating a Remote Workstation requires the use of certified cryptographic tools as part of the Moscow Exchange Electronic Data Interchange (EDI) System, the User must follow the EDI Rules and other regulations of the Technical Center on electronic data interchange when transmitting data via a public communication channel.

2.4 Form and format of electronic documents sent via a Remote Workstation to deliver User's orders and/or order cancellation instructions that are going to be submitted to the TC SHC are determined by software used by the User.

3. Technical specifications for Technical Access via Refinitiv/Bloomberg Workstations

3.1 Refinitiv/Bloomberg Workstations are connected to the Exchange directly by using systems developed by Refinitiv/Bloomberg. The systems are enabled and operated in accordance with the rules of use of Refinitiv/Bloomberg software.

3.2 Technical support needed to keep Refinitiv/Bloomberg Workstations connected is provided directly by Refinitiv/Bloomberg's technical support services pursuant to terms and conditions of the agreement between the User and Refinitiv/Bloomberg.

4. Technical specifications for Technical Access via User Software

4.1 A connectivity scheme applied to User Software must be in line with one of network connectivity schemes prescribed by MOEX for connection to the TC SHC (please refer to https://www.moex.com/s653) and one of the API connectivity options (please refer to section 'DMA interfaces' at https://www.moex.com/s346).

4.2 The User undertakes to meet MOEX Technical Center Requirements for User Software and connection thereof to the TC SHC available at https://fs.moex.com/files/10663.

4.3 Any User Software available for connection to the TC SHC and Subsystems is subject to certification pursuant to the Moscow Exchange Procedure for User Software Certification available at https://www.moex.com/s745.

4.4 The User should choose Software and enter into an agreement with the Software provider, or develop a system that meets MOEX Technical Center requirements for User Software on its own or in conjunction with a third-party developer, and then get it certified according to the Rules.

4.5 The User Software is subject to testing within the Technical Center's testing environment. It is tested by the User itself or an authorized developer, by using the User's test ID(-s).

4.6 The User undertakes to connect only certified User Software to the TC SHC and notify the Technical Center of the software so connected.

4.7 The User Software must be operated strictly in compliance with provisions of these Rules for the rules of connection of User Software to the TC SHC as well as instruction and guides developed by the software provider and agreed with the Technical Center in terms of data protection.

4.8 The User is fully responsible for any actions made in the TC SHC by using the User Software as well as in relation to running the User Software.

4.9 If running the User Software requires the use of certified cryptographic tools as part of the Moscow Exchange Electronic Data Interchange (EDI) System, the User must follow the EDI Rules and other regulations of the Technical Center on electronic data interchange when transmitting data via a public communication channel.

4.10 If cryptographic tools of the Moscow Exchange EDI System are used in conjunction with the User Software, cryptographic keys used for that software must have scope defined in the Terms of Integrated IT Service.

4.11 The User is responsible for disclosing, reproducing and/or disseminating any information related to operation of the TC SHC and covered by professional secrecy, as well as for disclosing, reproducing and/or disseminating any other information related to operation of the TC SHC, in cases where the User has not been authorised to disclose, reproduce and/or disseminate that information by the Technical Center.

4.12 The User is fully responsible for actions of its Clients made by using the User Software, also for disclosing, reproducing and/or disseminating by Clients any information related to operation of the TC SHC and covered by professional secrecy, as well as for disclosing, reproducing and/or disseminating by Clients any other information related to operation of the TC SHC that was made available to them as a result of their use of the User Software, except where the Client has been authorised to disclose, reproduce and/or disseminate that information by the Technical Center.

4.13 The Technical Center is not liable for any failure of the User Software to operate and/or for actions made by the User or its Clients by using the User Software including mistakes and violations made by the User in its capacity as Trading Member/Participant at order entry.

4.14 If the User provides access to information on operation of the TC SHC to its Clients in their use of the User Software, it shall enter into agreements (supplementary agreements) with the Clients stipulating the Client’s obligation not to disclose, reproduce and/or disseminate any information related to operation of the TC SHC and covered by professional secrecy, as well as disclose, reproduce and/or disseminate any other information related to operation of the TC SHC that was made available to the Client as a result of its use of the User Software, except where the Client has been authorised to disclose, reproduce and/or disseminate that information by the Technical Center.

4.15 The Integrated IT Service Administrator is responsible for operation of the User Software on the part of the User.

5. Technical specifications for Technical Access via Corporate Marketplace (CM)

5.1 Technical Access via the CM is only provided to Trading Members and/or Clearing Members of the FX Market and Precious Metals Market and/or Trading Members of the Deposit Market and/or Trading Members of the Credit Market and/or Trading Members of the Derivatives Market.

5.2 The CM service allows Trading Members and/or Clearing Members to implement the following features:

5.2.1 The User is given single Technical Access to TC SHC Sub-Systems which were made previously available to the User according to the procedure set forth in the admission rules for the relevant market and/or clearing rules;

5.2.2 Users within a Holding are given Single Technical Access to TC SHC Sub-Systems which were made previously available to every User according to the procedure set forth in the admission rules for the relevant market and/or clearing rules, acting via a representative with the login received at registration at passport.moex.com. In this case, orders and other electronic documents of every Holding member used within the relevant TC SHC Sub-System are signed with the basic electronic signature of the Trading Member and/or Clearing Member.

5.3 The TC SHC Sub-System functionality accessible via the CM is limited. Details on currently available functionality are at https://www.moex.com/a1819. The User will be informed of any further functionality made available in the TC SHC Sub-System in one of the manners set forth in clause 13.6 of the Terms of Integrated IT Service.

5.4 To receive the CM service, a member must be registered on passport.moex.com and have the appropriate terminal Technical Access ID allowing Technical Access to the relevant TC SHC Sub-Systems.

5.5 The CM service is provided through the application process. The recommended application form is available on the Moscow Exchange website at http://moex.com/a1819.

The application shall contain the names of the TC SHC Subsystems, Technical Access ID, the login received at registration on the passport.moex.com, token (if any) and other information. The application may be submitted both in hard copy and in the form of an electronic document using the Moscow Exchange EDI System. TC shall process the application within the period set out in clause 10.2 below, and, based on the results of the check, shall send a notice to the User via the EDI System. When submitting the applications from the Trading Members and/or Clearing Members belonging to the Holding, each of such applications shall contain the same personal login of the representative obtained upon registration on the website passport.moex.com. Every application from Trading Members and/or Clearing Members in a Holding shall specify the representative’s same personal login obtained at registration on passport.moex.com.

5.6 Users with single Technical Access via the CM are required to have tokens (hardware or software devices) and/or data cryptographic protection tools providing an additional level of security in the authentication process. Token and other related services are provided to the User based on an Integrated Technology Service Agreement or Technical Centre’s Information Technology Service Agreement Technical Centre’s Information Technology Service Agreement. The User receives cryptographic protection tools when signing the Agreement on Participation in the Moscow Exchange EDI System.

5.7 If for the login received upon registration at passport.moex.com, when accessing the clearing terminal and/or web clearing within the FX Market and Precious Metals Market Clearing System, a cryptographic electronic signature tool corresponding to a certain electronic signature verification key certificate (the ESVKC) is already used as an additional security factor at authentication, this ESVKC shall be used for access to the CM service as well.

Disconnection from the clearing terminal and/or web clearing does not stop the use of the relevant ESVKC for access to the CM.

The Trading Members and/or Clearing Members shall not be entitled to use the token as the second factor of authentication protection for access to the CM, if the cryptographic key corresponding to a certain ESVKC is used as the second factor of authentication protection for access to the clearing terminal and/or web clearing.

The details of the ESVKC, the cryptographic key of which is used for access to the Clearing Centre, shall be specified in the application for connection to the CM.

5.8 A Trading Member and/or Clearing Member shall be entitled to use the features of both the single Technical Access implemented through the CM and the features of the Technical Access ID, by using software intended for connection to the TC SHC Subsystems of the relevant markets.

5.9 Special aspects of the relation between Technical Access IDs and logins of the User (a representative of the Users) obtained at registration on passport.moex.com (the "Login”):

5.9.1 one login of a Trading Member and/or the Clearing Member may be linked only to one Technical Access ID in each of the TC SHC Subsystem to which the User has access;

5.9.2 one login of the representative of the Users involved in a Holding may be linked to one Technical Access ID of each User within those TC SHC Subsystems to which the Users have access; a representative in the CM shall be entitled to choose the User and the TC SHC Subsystems to which the Technical Access ID of the Trading Member and/or Clearing Member will have access at a particular time.

5.9.3 one login of a representative of Users being part of the Holding Company may be used for Technical Access via the CM, if a token is used as an additional security factor for authentication of such representative; if the same ESVKC and login are used, the Technical Centre is entitled not to provide Technical Access via the CM to a representative of Users being part of the Holding Company.

The restricting provisions in this section do not apply to the TC SHC Subsystem of the MOEX Derivatives Market.

6. Remote Workstation/Customer Software health check

6.1 Remote Workstation and/or Customer Software health checks are performed only for the Equity & Bond, FX, Precious Metals, Derivatives and Standartised OTC Derivatives Markets.

6.2 At the User’s request, the Technical Center performs (during the trading hours of the Derivatives, FX, Precious Metals, Standartised OTC Derivatives and Equity & Bond Markets) health checks of a remote Workstation, Customer Software and/or a Client of the User and provides automatic deletion of active orders (including orders submitted based on the instructions of the Client connected to the Instruction Processing Subsystem allowing the use of the Sponsored Access IDs) if the Remote Workstation, Customer Software and/or the Client (save for Refinitiv/Bloomberg workstations) is found to be not operative, or if a certain trading ID/Sponsored Access ID is suspended in terms of order submission, amendment and cancellation.

6.3 The User requests to enable/disable Remote Workstation and/or Customer Software health checks on the relevant market when completing an application form for identifiers which is available on the Technical Center's website at http://moex.com/a1819.

6.4 Upon receiving the User's request to enable Remote Workstation and/or Customer Software health checks, the Technical Center enables the health check and active order automatic cancellation features for the User within five (5) business days provided that the User's Remote Workstation/Customer Software meets the Technical Center's requirements published at http://moex.com/a1819.

6.5 After the features are activated by the Technical Center, it may cancel automatically active orders in the TC SHC during the trading hours of the relevant market, if a health check with the use of a certain trading ID is not possible on that market for the remote Workstation and/or Customer Software. Heath checks for Remote Workstations and/or Customer Software are performed according to the procedure of the Technical Center.

6.6 If a health check initiated based on the User's standing request is not possible for the client-side software, an authorised representative of the Technical Center notifies the User of its inability to cancel the User's orders, in one of the ways set out in Paragraph 13.6 of the Terms.

6.7 If active orders supposed to be cancelled by the Technical Center have been already filled, they are not available for cancelation by the Technical Center.

6.8 The User may request that the functionality for health checks and automatic cancellation of active orders be disactivated in respect of the certain market by making the necessary marks in the application on identifiers which is performed by the Technical Center within five (5) business days.

6.9 The Technical Center accepts no responsibility for losses the User may incur as a result of Remote Workstation and/or Customer Software health checks and cancellation of its active orders.

7. Technical specifications for Technical Access to the Instruction Procession Subsystem

7.1 Remote Workstation and Customer Software employed by the User to perform technical access to the Instruction Processing Subsystem of a certain market, must meet the requirements set out in these Rules and other regulations of the Technical Center.

7.2 If the User provides Technical Access to the Instruction Processing Subsystem to its Clients under the Integrated IT Service Terms, it must ensure that requirements set out in the Integrated IT Service Terms, these Rules and other Technical Center's regulations are met, as well as it is fully responsible for a failure to comply with those requirements for hardware and software used by the User's Client to perform Technical Access to the subsystem.

7.3 At the request of the Technical Center, the User must submit documents needed to certify the compliance of the hardware and software with the requirements set out in the Integrated IT Service Terms, these Rules and other regulations of the Technical Center.

8. Recommendations on, and minimum requirements for parameters of hardware used in facilitating Technical Access to the TC SHC

8.1 Recommendations on and minimum requirements for the User's software and hardware, as well as requirements for channel bandwidths are set out in the Moscow Exchange Requirements for Customer Software Connection to the TC SHC which are available at https://www.moex.com/s745, as well as in the Recommendations on, and Minimum Requirements for Parameters of Hardware used for Technical Access to Moscow Exchange Trading and/or Clearing Systems which are available at http://fs.moex.com/files/10663.

8.2 All Users that are trading members:

- Are recommended to have a backup connection to the Primary Data Center of the Technical Center. To facilitate backup connectivity, the Internet or a leased line provided by a telecom carrier other than the User's principal telecom carrier (the list of authorised providers of Moscow Exchange is available at https://www.moex.com/a1224?utm_source=www.moex.com&utm_term=784-66) may be used;
- Are required to have a backup connection to the Disaster Recovery Data Center of the Technical Center.

  Users that are trading members connecting via the colocation facility and/or ConnectME have a backup connection to the Disaster Recovery Data Center over the Internet or ConnectME.

  Users that are trading member connecting via the universal scheme with backup over various providers, do not need to have a backup connection to the Disaster Recovery Center.

8.3 All Users are recommended to organize their own telecommunication infrastructure via leased lines provided by two different providers that are accredited partners of Moscow Exchange, for connection to the TC SHC.

8.4 The User must notify the Technical Center of the connection method it employs to connect to the Disaster Recovery Data Center at least once a year.

9. Warranty maintenance

9.1 To get warranty service specified in Section 3 of the Integrated IT Service Terms, the User should contact the Technical Center's support service by phone or emails published at https://www.moex.com/s373.

9.2 Inquiries from Users are accepted and processed during the trading hours on the TC's business days. The trading schedule is available at https://www.moex.com/s371.

10. Issue and cancellation of Technical Access IDs

10.1 The User is given a Technical Access ID through an application form for receiving/changing a technical access ID that is described in Paragraph 2.2 of the Integrated IT Service Terms if the User's representative who signed such application has the necessary authorisation.

10.2 In the Application, the User undertakes to specify the full name of the person using the Technical Access ID in accordance with its functionality; for services using an electronic signature verification key certificate (ESVKC), it is necessary to ensure that the personal data of the ESVKC holder and the full name of the Technical Access ID User match those specified in the Application; personalisation of the ID does not apply to Sponsored Access ID and technological identifiers. For services using passport.moex, it is necessary to ensure that the full names of Technical Access ID Users on several markets of Moscow Exchange used with one passport.moex, as well as the full name of the Service User, match.

10.3 Existing Users may switch to personalised Technical Access IDs by submitting an application to change the Technical Access ID, additionally specifying the full names of representatives of Trading Members and/or Clearing Members which are users of the IDs, with a link to the relevant ESVKC (if necessary). In the absence of the Application for Technical Access ID change before 01 January 2022, the Parties agree that the User's representative performing actions in the relevant SHC Subsystem is the sole executive body of the User specified in the Unified State Register of Legal Entities, which is publicly available.

10.4 Identification and authentication of the User's representative working in the SHC Subsystems using personalised Technical Access IDs is done by recognising and verifying in the TC SHC the information on the Technical Access ID, unique access password to such ID, and, if necessary, by the ESVKC issued for a particular User's representative. The procedure of assignment of the Technical Access ID and subsequent authentication and/or identification of the User's representative allows to ensure confirmation that actions in the TC SHC Subsystems, including drafting and signing of electronic messages with an electronic signature, are performed by an authorised person with authentication of the message sender (if necessary). The procedure for obtaining the password for Technical Access ID registration is given in this Section.

10.5 Application by the Trading Member and/or the Clearing Member of the Technical Access IDs allows to use the functionality of the relevant TC SHC Subsystem and to sign electronic messages, including electronic documents, including when submitting/modifying/cancelling orders in accordance with the Organised Trading Rules and/or the Clearing Rules, with a basic electronic signature of the User's authorised representative. The Technical Access ID is given in the electronic message (electronic document). The password for registration of the Technical Access ID in the TC SHC is a basic electronic signature key. The forms and formats of electronic documents that Users are entitled to sign with a basic electronic signature are provided for by the internal documents of the market operator and/or are determined by means of specialised software of the Technical Centre. Electronic messaging shall be carried out in accordance with the provisions of the Civil Code of the Russian Federation, Federal Law "On Electronic Signature" No. 63-FZ dated 06 April 2011, these Rules, as well as taking into account the information protection requirements established by the Regulation of the Bank of Russia No. 757-P dated 20 April 2021 "On Establishing Mandatory Requirements for Non-Credit Financial Organisations to Ensure Information Protection when Operating in the Financial Markets to Prevent Illegal Financial Transactions".

10.6 A technical access ID is given to the User, or parameters of the previously given ID are changed within five (5) business days after receiving the application by the Technical Center, or after the User was admitted to trading/transacting and/or clearing service on the relevant market, provided that the Technical Center has no concerns about the application and all technical facilities are available.

10.7 The User receives a rejection/ID scope change notification, if applicable, according to the established procedure within five (5) business days after receiving the application by the Technical Center.

10.8 The Technical Center terminates a technical access ID on the User's initiative within five (5) business days after receiving the relevant application described in Paragraph 2.2 of the Integrated IT Service Terms from the User.

10.9 If the User loses its access to trade on one or more Moscow Exchange's market, all trading rights associated with the User's Technical Access ID as well as all its Technical Access IDs intended exclusively for trading on specific markets, are terminated.

10.10 If the User loses its access to the clearing service on one or more Moscow Exchange's market, all clearing rights associated with the User's Technical Access ID as well as all its Technical Access IDs intended exclusively for the clearing service on specific markets, are terminated.

10.11 If the User loses its access to the trading and clearing services on one or more Moscow Exchange's market, all its Technical Access IDs registered on the relevant markets are terminated, except for IDs registered in the Clearing System of the Equity & Bond Market, Deposit Market and Credit Market.

10.12 Each Clearing Member, who has entered into the Clearing Service Agreement with CCP NCC, is provided (upon application from the User and regardless of whether the Clearing Member is admitted to clearing services on the Equity & Bond Market) with the Technical Access ID with authority to make clearing operations on the Equity and Bond Market. Such Technical Access ID allows the Clearing Member to use the CCP NCC services, which are not related to execution of trades on the Moscow Exchange markets, set out in the CCP NCC Clearing Rules. In case the Clearing Member is not admitted to clearing service on the Equity & Bond Market, other functions of the Clearing System of the Equity & Bond, Credit and Deposit Markets are not available to the Clearing Member. The CCP NCC's services not related to execution of trades on MOEX's markets and set out in the CCP NCC Clearing Rules, refer to functionality of the Clearing ID, which is billed in accordance with the Tariffs depending on the number and type of the Technical Access IDs in use.

10.13 If the User wishes to change functionality scope of its Technical Access ID (trading, view-only, clearing, or sponsored access) or the type of the ID (API or terminal), it must terminate its current ID and get a new one paying the registration fee according to the Tariffs.

10.14 If the User needs to limit/change the scope of rights or other characteristics associated with its Technical Access ID, it should apply according to Paragraph 2.2 of the Integrated IT service Terms to the Exchange.

10.15 Suspension of a Technical Access ID at the User's request is not allowed.

10.16 The User is fully responsible for the use of Technical Access IDs received.

10.17 The Users who are Trading Members and/or Clearing Members of the Derivatives Market shall be provided with a unique password. The Technical Centre shall provide the primary password to the Trading Members and/or Clearing Members of other markets. In case of receipt of the primary password for Technical Access ID registration in TC SHC, the representative of the User using the ID shall change the password or submit an application to the Technical Centre for password change. In case the User fails to fulfil the obligation stipulated by this clause to change the primary password for a new, more reliable password not known to third parties, the Technical Centre shall not be liable for unauthorised access to the TC SHC by unauthorised persons.

10.18 If the User loses its password, it may contact the Technical Center to get a new one.

10.19 The primary and/or individual password generated by the Technical Centre shall be delivered to the User by sending it by e-mail through mailboxes opened to the User on the mail server of the Technical Centre for receiving electronic documents.

10.20 The Technical Center may unilaterally block and/or suspend a Technical Access ID if it has detected the User's attempts to gain unauthorized access to the TC SHC, the coincidence of the Technical Access ID owner and the User's representative performing actions in the TC SHC Subsystems is not confirmed, or other circumstances have occurred that prevent the normal operation of the TC SHC.

10.21 Unblocking Technical Access ID

Upon expiration of the grounds for Technical Access ID blocking, the User has the right to submit to the Technical Centre an application for Technical Access ID unblocking in the form of a telephone message (the "Application for Technical Access ID unblocking").
On behalf of the User, the sole executive body or other authorised employee may submit the Application for unblocking of the Technical Access ID, provided that the data on the abovementioned persons are contained in the Legal Entity Details Form provided in accordance with the Admission Rules. The Application for Unblocking shall contain the following details:
a) surname, first name, patronymic (if any) and telephone number of the person applying for unblocking of the Technical Access ID;
b) code word coinciding with the code word specified in the Legal Entity Details Form;
c) Technical Access ID to be unblocked.

If the details of the Application for Unblocking are correct, the Technical Centre shall unblock the Technical Access ID after confirming the termination of the grounds for blocking and availability of technical capability.
If the details of the Application for Unblocking are incorrect or the circumstances that served as grounds for blocking of the ID continue to exist, such Application shall be rejected, of which the Technical Centre shall inform the person who submitted the Application by means of telephone communication.

The User has the right to unlock the Technical Access ID via code word 1 (one) time per day. The repeated unlocking of the Technical Access ID on the same day can be performed on condition of submitting a letter made up in the form available on the Technical Centre's websitewww.moex.com.