Approved
MOEX Information Security
Order No. МБ-ЗИ/П-1 as of 7 April 2020

Telecommunication services procedures

MOEX Information Security

These procedures may be amended or supplemented at any time. The version in effect is available on the Operator website.

The following terms and definitions are used throughout the text below alongside the terms and definitions set out in the Telecommunications Services Rules of the MOEX Information Security Limited Liability Company (the "Operator")

Structured cabling system (SCS) - a set of cables and switching equipment, used to organize local computer networks. It includes cables between cabinets, patch cords, patch panels, mounting equipment, etc.;

MOEX Trade Network– a dedicated computer network that gives technical access to the trading, clearing and payments systems, as well as to depositary and auxiliary systems and services of entities within the Moscow Exchange Group;

Production and Game systems access network segment – logically and physically isolated part (segment) of the Operator's Network within the Co-location Facility designed to enable technical access to settlement, depository and other services within the production and gaming systems;

UAT systems access network segment – logically and physically isolated part (segment) of the Operator's Network within the Co-location Facility designed to enable technical access to the testing systems within the MOEX Trade Network;

Internet-access network segment - logically and/or physically isolated part (segment) of the Operator's network, designed for the Internet access (telematics telecommunication service delivery).

PTP clock synchronization network segment – logically and/or physically isolated part (segment) of the Operator's network designed for time synchronization with MOEX PTP Grandmaster using the Precision Time Protocol (PTP).

1. Network connectivity requirements

1.1 Connection of Client's equipment to the Operator's network

1.1.1 Connection of the Client's network equipment to the Operator's network is provided in accordance with the requirements specified in paragraphs 1.6 and 1.8, connection of the Client's server equipment is provided in accordance with requirements specified in paragraphs 1.3 and 1.5.

1.1.2 The following types of the connection services to the Exchange network are possible:

- Access to the production and game systems network segment;
- Access to the test system network segment;
- Access to the PTP clock synchronization network segment.

1.1.3 Combination of connections to production & game systems segment and test systems segment on a single device is possible, however connections to different network segments should use

different dedicated ports (pair of ports).

1.2 Connection of Client's equipment to the Internet

1.2.1 Connection of network equipment to the Internet is provided in accordance with requirements specified in p. 1.7, connection of server equipment is provided in accordance with requirements specified in p. 1.4.

1.2.2 Combination of connections to the Internet-access network segment, Production and Game systems network segment, Test systems network segment on the same device is allowed; each network segment requires different dedicated port (pair of ports).

1.3 Server equipment connection to Operator's equipment in Production and Game systems access segment

1.3.1 Server equipment connection to production and game systems network is provided through the Operator's equipment using 10 Gbit/s and 1 Gbit/s ports.

1.3.2 Server equipment is connected to the Operator's equipment by using a pair of ports (two ports for each connection) in a redundant group mode (LACP, IEEE 802.3AX/IEEE 802.3ad). The Operator provides ports in each pair on two different devices.

1.3.3 Network interface pairs on the Client's server equipment used for connection to the Operator's equipment should have trunking configured (IEEE 802.1q) for redundancy (LACP, IEEE 802.3AX / IEEE 802.3ad). The Client's ports in each pair must be in Active-Active mode.

1.3.4 LACP group should be configured with 30 seconds timeout.

1.3.5 The Client's server equipment is connected to the Operator's equipment with cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.3.6 SFP modules (if needed) for connections on the Side of the Operator are provided by the Operator; for Client-side connections are provided by the Client.

1.3.7 Connections to 10 Gbit/s ports on the Operator equipment are done in accordance with 10GBASE-SR standard with duplex multimode fiber cables with LC-LC connectors and 10GBASE-SR modules. The Client at its premises may use 10GBASE-SR modules on network interfaces with SFP+ ports or QSFP ports with SFP+ adapter modules.

1.3.8 Connections to 1 Gbit/s ports on the Operator's equipment are done in accordance with 1000BASE-T/1000BASE-TX standard with copper UTP Cat5e/Cat6 cables with RJ45 connectors. The client can also use network interfaces with RJ45 or SFP standard connectors using 1000BASE-T standard modules.

1.3.9 The bandwidth and duplex port mode on the Client equipment must be set to "auto".

1.3.10 To be Connected to the Operator's network, the Client provides the Operator with the appropriate private range /24 networks for each Client for internal use (RFC 1918) which should be used for specific services obtained by the Client as part of its Colocation IT Services Agreement with Public Joint Stock Company Moscow Exchange and the Operator reserves the address ranges for the Production and Game system segments access.

1.3.11 The level of broadcast traffic received from the Client equipment should not exceed 2 Mbit/s.

1.3.12 In each connection, the Operator sends and receives traffic to/from specific IP-addresses allocated for the Client as part of the services ordered, provided that these IP-addresses are in the address ranges reserved for the Client for using them within the Production and Game systems network segment.

1.4 Server equipment and management interfaces connection to Operator's equipment in the Internet-access segment

1.4.1 Server equipment and dedicated management interfaces (mgmt-port) of the network devices are connected to the Internet-Facing Segment through the Operator's equipment using 1 Gbit/s ports on the side of the Operator.

1.4.2 The server hardware is connected to the Operator's equipment by using a pair of ports (two ports for each connection) in a redundant group mode (LACP, IEEE 802.3AX/IEEE 802.3ad). The Operator provides ports on two different devices in each pair.

1.4.3 Network interface pairs on the Client's server equipment used for connection to the Operator's equipment must have network group (LACP, IEEE 802.3AX / IEEE 802.3ad) configured. Each pair of ports on the Client side should be set to Active-Active mode.

1.4.4 LACP group should be configured with 30 seconds timeout.

1.4.5 Connection of management interfaces for Client equipment management modules (HP ILO Advanced, IBM RSA, DELL iDRAC, IPMI, etc.) with a single dedicated control module interface 100BASE-TX/1000BASE-TX is done through one port on the Operator's side. In this case the network group mode is not configured and requirements set out in p. 1.4.2, 1.4.3 and 1.4.4 are not applicable.

1.4.6 The Client's server equipment is connected to the Operator's equipment with cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.4.7 SFP modules (if needed) for connections on the Side of the Operator are provided by the Operator; for Client-side connections are provided by the Client.

1.4.8 Connections to 1 Gbit/s ports on the Operator's equipment are done in accordance with 1000BASE-T/1000BASE-TX standard with copper UTP Cat5e/Cat6 cables with RJ45 connectors. The client can also use network interfaces with RJ45 or SFP ports with 1000BASE-T standard modules.

1.4.9 The bandwidth and duplex port mode on the Client equipment must be set to "auto".

1.4.10 IP addresses and configurations to connect to the data network are provided by the Operator upon the connectivity service order execution.

1.4.11 The level of broadcast traffic received from the Client equipment should not exceed 2 Mbit/s.

1.4.12 The Operator reserves certain address ranges (/24) out of RFC 1918 for the Client.

1.4.13 At every connection node, the Operator sends and receives traffic to/from specific IP-addresses allocated for the Client as part of the services ordered, provided that these IP-addresses are within the address ranges reserved for the Client for using them within the Internet-Facing Network Segment.

1.4.14 IP addresses are given by the Operator as part of the service order. To get IP addresses and setup, the Client must complete an order form given in Appendix 4. When giving the addresses, the Operator provides information necessary to configure VLAN, subnet mask, broadcast address and default route (if needed).

1.4.15 Network connection between the Client's equipment and Internet is secured by the network firewalls of the Operator according to the configuration agreed with the Client.

1.4.16 Outgoing connections from network ports of the Client's independent equipment management modules (HP ILO Advanced, IBM RSA, DELL DRAC, IPMI, etc.) to Internet are forbidden on the Operator's network devices.

1.4.17 It is not allowed to use an access policy that allows Internet inbound connections to the Client's equipment via standard remote management ports (22/tcp, 23/tcp, 3389/tcp) and in case of independent management modules additional ports (80/tcp, 443/tcp, 5900/tcp) without limiting the range of Internet IP addresses.

1.5 Server equipment connection to Operator's equipment in the UAT systems access segment

1.5.1 The server equipment is connected to the UAT systems access segment through the Operator's equipment using 10 Gbit/s and 1 Gbit/s ports on the Operator's side.

1.5.2 The recommended method of the server hardware connection to the Operator's equipment is by using a pair of ports (two ports for each connection) in a redundant group mode (LACP, IEEE 802.3AX/IEEE 802.3ad). The Operator provides ports on two different devices in each

pair. It is allowed, but not recommended to use single port to connect the server equipment to the Operator's equipment.

1.5.3 The Client's server equipment is connected to the Operator's equipment with cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.5.4 Network interface pairs on the Client's server equipment used for connection to the Operator's equipment should have trunking configured (IEEE 802.1q) for redundancy (LACP, IEEE 802.3AX / IEEE 802.3ad). In case one port is used to connect to the Operator's equipment, the port must be configured to IEEE 802.1q trunk.

1.5.5 LACP group should be configured with 30 seconds timeout. The Client's ports in each pair must be set to Active-Active mode.

1.5.6 SFP modules (if needed) for connections on the Side of the Operator are provided by the Operator; for Client-side connections are provided by the Client.

1.5.7 Connections to 10 Gbit/s ports on the Operator equipment are done in accordance with 10GBASE-SR standard with duplex multimode fiber cables with LC-LC connectors and 10GBASE-SR modules. The Client at its premises may use 10GBASE-SR modules on network interfaces with SFP+ ports or QSFP ports with SFP+ adapter modules.

1.5.8 Connections to 1 Gbit/s ports on the Operator's equipment are done in accordance with 1000BASE-T/1000BASE-TX standard with copper UTP Cat5e/Cat6 cables with RJ45 connectors. The client can also use network interfaces with RJ45 or SFP standard connectors using 1000BASE-T standard modules.

1.5.9 The bandwidth and duplex port mode on the Client equipment must be set to "auto".

1.5.10 To be Connected to the Operator's network, the Client provides the Operator with the appropriate private range /24 networks for internal use (RFC 1918) which should be used for specific services obtained by the Client as part of its Colocation IT Services Agreement with Public Joint Stock Company Moscow Exchange, and the Operator reserves these address ranges for use in UAT systems access network segment.

1.5.11 The level of broadcast traffic received from the Client equipment should not exceed 2 Mbit/s.

1.5.12 In each connection, the Operator sends and receives traffic to/from specific IP-addresses allocated for the Client as part of the services ordered, provided that these IP-addresses are in the address ranges reserved for the Client for using them within the UAT systems access network segment.

1.6 Connection of network equipment to Operator's equipment in Production and Game systems access segment

1.6.1 The network equipment is connected to the Production and Game systems access segment through the Operator's equipment using 10 Gbit/s ports on the Operator's side.

1.6.2 The network equipment is connected to the Operator's facilities by pair of ports (two ports for each connection). The Operator provides ports on two different devices in each pair. The Client is recommended to have ports on two different devices in each pair; it is also allowed to have ports on a single device in each pair.

1.6.3 The Client's server equipment is connected to the Operator's equipment with cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.6.4 SFP modules (if needed) for connections on the Side of the Operator are provided by the Operator; for Client-side connections are provided by the Client.

1.6.5 Connections to 10 Gbit/s ports on the Operator equipment are done in accordance with 10GBASE-SR standard with duplex multimode fiber cables with LC-LC connectors and 10GBASE-SR modules. The Client at its premises may use 10GBASE-SR modules on network interfaces with SFP+ ports or QSFP ports with SFP+ adapter modules.

1.6.6 Network interfaces on the Client equipment used for connection to the Operator must operate in L3 mode, have unique MAC addresses and do not have interim elements which allow changing the switching logic.

1.6.7 The bandwidth and duplex port mode on the Client equipment must be set to "auto".

1.6.8 To be Connected to the Operator's network, the Client provides the Operator with the appropriate private range /24 networks for internal use (RFC 1918) which should be used for specific services obtained by the Client as part of its Colocation IT Services Agreement with Public Joint Stock Company Moscow Exchange, and the Operator reserves these address ranges for use in Production and Game systems access network segment.

1.6.9 The Client's network equipment used to connect to the Operator must support the BGP dynamic routing protocol.

1.6.10 BGP dynamic routing protocol is used between the Client's network equipment and the Operator's network facilities. Other dynamic routing protocols as well as static routing protocols are not used.

1.6.11 For connection configuration the Client should use the network settings provided by the Operator, i.e. IP addresses of the peering network, BGP timings, Operator's AS number, AS number used by the Client which is within the internal use range (AS64512-AS65534). At the Client's request, the Client may use its own public AS number.

1.6.12 At every connection node of the Client network equipment, the Operator accepts the network subnet prefixes from /32 to /24 from the address space reserved for Client.

1.6.13 On every connection the Operator sends and receives traffic to/from specific IP-addresses allocated for the Client as part of the ordered services, provided that these IP addresses are in the address space reserved for the Client for using them within the Production and Game systems access segment and announced over this connection by the Client's network equipment towards the Operator's network equipment.

1.6.14 It is possible to use administrative methods of route extension to set preferred route selection between different Client connections.

1.6.15 The Client is allowed to use IP addresses from its reserved address space without notifying the Operator. In this case, the Operator does not accept and send traffic from/to these addresses.

1.6.16 If the Client uses overlapping IP address ranges for its network equipment and server equipment connections, the absolute priority for inbound and outbound traffic from/to a specific IP address will be set for network equipment connection if this network equipment announces this IP address within /24 to /32 length prefix, otherwise the priority will be set for the server connection.

1.6.17 If the Client uses overlapping IP ranges for different network equipment connections, the absolute priority for inbound and outbound traffic from/to a specific IP address will be set for network equipment announcing this IP address within the most specific prefix.

1.6.18 To receive multicast service, the Client equipment should support PIM protocol.

1.6.19 Client network equipment facing the Operator equipment should have LLDP protocol enabled (if supported).

1.6.20 Client network equipment facing the Operator equipment should have BFD protocol enabled (if supported).

1.7 Connection of network equipment to the Operator's equipment in Internet-access segment

1.7.1 Client network equipment or their dedicated management interfaces (mgmt-port) are connected to the Internet-access network segment through the Operator's equipment with 1 Gbit/s ports.

1.7.2 Network equipment connection to the Operator is done by pair of ports (two ports for each connection). On the Operator's side, each pair of ports is allocated on two different network devices. On the Client's side, it is recommended to terminate each link on different network devices, however having 2 links connected to a single network device is also allowed.

1.7.3 Network device dedicated management interfaces (mgmt port) are connected via one port on

the Operator's equipment. In this case, the BGP dynamic routing protocol is not configured and paragraphs 1.7.7, 1.7.10, 1.7.11 and 1.7.12 do not apply.

1.7.4 The Client's server equipment is connected to the Operator with cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.7.5 SFP modules (if needed) for Operator-side connections are provided by the Operator, for Client-side connections are provided by the Client.

1.7.6 Connections to 1 Gbit/s ports on the Operator equipment are done in accordance with 1000BASE-T/1000BASE-TX standard with copper UTP Cat5e/Cat6 cables with RJ45 connectors. The client can use network interfaces with RJ45 ports or SFP standard connectors with 1000BASE-T standard modules.

1.7.7 Network interfaces on the Client equipment used for connection to the Operator must operate in L3 mode, have unique MAC addresses and do not have interim elements which allow changing the switching logic.

1.7.8 Bandwidth and duplex port mode on the Client equipment should be set to "auto".

1.7.9 IP addresses and peering network settings are provided by the Operator as part of the connectivity service order.

1.7.10 The Client's network equipment used to connect to the Operator must support the BGP dynamic routing protocol.

1.7.11 BGP dynamic routing protocol is used between the Client's network equipment and the Operator's network facilities. Other dynamic routing protocols as well as static routing protocols are not used.

1.7.12 For connection configuration the Client should use the network settings provided by the Operator, i.e. IP addresses of the peering network, BGP timings, Operator's AS number, AS number used by the Client which is within the internal use range (AS64512-AS65534). At the Client's request, the Client may use its own public AS number.

1.7.13 The Operator provides separate private range /24 networks for each Client for internal use (RFC 1918) which should be used for specific services.

1.7.14 For each Client network equipment connection the Operator accepts of the network subnet prefixes from /32 to /24 from the address space reserved for Client.

1.7.15 For each connection the Operator sends and receives traffic to/from specific IP-addresses allocated for the Client for provision of specific services, if such IP addresses have been enabled for the Client to be used to access Internet network segments and which are announced over this connection by the Client network equipment.

1.7.16 It is possible to use administrative methods of route extension to set preferred route selection between different Client connections.

1.7.17 The Client is allowed to use IP addresses from its reserved address spaces without notifying the Operator. In this case, the Operator does not accept and send traffic from/to these addresses.

1.7.18 If the Client uses overlapping IP address ranges for its network equipment and server equipment connections, the absolute priority for inbound and outbound traffic from/to a specific IP address will be set for network equipment connection if this network equipment announces this IP address within /24 to /32 length prefix, otherwise the priority will be set for the server connection.

1.7.19 If the Client uses overlapping IP ranges for different network equipment connections, the absolute priority for inbound and outbound traffic from/to a specific IP address will be set for network equipment announcing this IP address within the most specific prefix.

1.7.20 IP addresses are provided by the Operator as part of the relevant connection services. To receive IP addresses and network configuration, the Client should fill out IP address allocation request as shown in Appendix 4.

1.7.21 Network connection between the Client equipment and the Internet is secured by the Operator firewalls in accordance with configuration agreed with the Client.

1.7.22 Outbound Internet connections from network device management interfaces (mgmt. port) are prohibited by the Operator.

1.7.23 It is not allowed to use an access policy that allows Internet inbound connections to the Client's equipment via standard remote management ports (22/tcp, 23/tcp, 3389/tcp) and in case of independent management modules additional ports (80/tcp, 443/tcp, 5900/tcp) without limiting the range of Internet IP addresses.

1.7.24 Client network equipment facing the Operator equipment should have LLDP protocol enabled (if technically possible).

1.8 Connection of network equipment to Operator's equipment in UAT systems access segment

1.8.1 Client network equipment is connected to the UAT systems access network segment through the Operator's equipment with 1 Gbit/s or 10 Gbit/s ports.

1.8.2 Network equipment connection to the Operator is done by pair of ports (two ports for each connection). The Operator provides ports on two different devices in each pair. It is allowed, but not recommended to use single port to connect the network equipment to the Operator's equipment. On the Client's side, it is recommended to terminate each link on different network devices, however having 2 links connected to a single network device is also allowed.

1.8.3 The Client's network equipment is connected to the Operator with cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.8.4 SFP modules (if needed) for Operator-side connections are provided by the Operator, for Client-side connections are provided by the Client.

1.8.5 Connections to 10 Gbit/s ports on the Operator equipment are done in accordance with 10GBASE-SR standard with duplex multimode fiber cables with LC-LC connectors and 10GBASE-SR modules. The Client at its premises may use 10GBASE-SR modules on network interfaces with SFP+ ports or QSFP ports with SFP+ adapter modules.

1.8.6 Connections to 1 Gbit/s ports on the Operator equipment are done in accordance with 1000BASE-LX standard with double multimode fiber cables with LC-LC connectors and 1000BASE-LX/LH modules.

1.8.7 Network interfaces on the Client equipment used for connection to the Operator should be configured in L3 mode.

1.8.8 To be Connected to the Operator's network, the Client provides the Operator with the appropriate private range /24 networks for internal use (RFC 1918) which should be used for specific services obtained by the Client as part of its Colocation IT Services Agreement with Public Joint Stock Company Moscow Exchange, and the Operator reserves these address ranges for use in UAT systems access network segment.

1.8.9 Bandwidth and duplex port mode on the Client equipment should be set to "auto".

1.8.10 The Client's network equipment used to connect to the Operator must support the BGP dynamic routing protocol.

1.8.11 BGP dynamic routing protocol is used between the Client's network equipment and the Operator's network equipment. Other dynamic routing protocols as well as static routing protocols are not used.

1.8.12 For connection configuration the Client should use the network settings provided by the Operator, i.e. IP addresses of the peering network, BGP timings, Operator's AS number, AS number used by the Client which is within the internal use range (AS64512-AS65534). At the Client's request, the Client may use its own public AS number.

1.8.13 At every connection node of the Client network equipment, the Operator accepts the network subnet prefixes from /32 to /24 from the address space reserved for Client.

1.8.14 On every connection the Operator sends and receives traffic to/from specific IP-addresses allocated for the Client as part of the ordered services, provided that these IP addresses are in the address space reserved for the Client for using them within the UAT systems access

segment and announced over this connection by the Client's network equipment towards the Operator's network equipment.

1.8.15 It is possible to use administrative methods of route extension to set preferred route selection between different Client connections.

1.8.16 The Client is allowed to use IP addresses from its reserved address space without notifying the Operator. In this case, the Operator does not accept and send traffic from/to these addresses.

1.8.17 If the Client uses overlapping IP address ranges for its network equipment and server equipment connections, the absolute priority for inbound and outbound traffic from/to a specific IP address will be set for network equipment connection if this network equipment announces this IP address within /24 to /32 length prefix, otherwise the priority will be set for the server connection.

1.8.18 If the Client uses overlapping IP ranges for different network equipment connections, the absolute priority for inbound and outbound traffic from/to a specific IP address will be set for network equipment announcing this IP address within the most specific prefix.

1.8.19 To receive multicast service, the Client equipment should support PIM protocol.

1.8.20 Client network equipment facing the Operator equipment should have LLDP protocol enabled (if supported).

1.8.21 Client network equipment facing the Operator equipment should have BFD protocol enabled (if supported).

1.9 Equipment connection to the Operator's equipment in the Precise time service access segment.

1.9.1 Client equipment is connected to the Precise time service access segment using PTP protocol (Precision Time Protocol) and via the Operator's equipment with the use of fiber and copper network ports.

1.9.2 Equipment connection to the Operator is done by pair of ports (two ports for each connection) translating separate PTP domain information. The Operator provides ports on two different devices in each pair. It is allowed, but not recommended to use single port to connect the equipment to the Operator's equipment. On the Client's side, it is recommended to terminate each link on different devices, however having 2 links connected to a single device is also allowed.

1.9.3 The Client's equipment is connected to the Operator with cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.9.4 SFP modules (if needed) for Operator-side connections are provided by the Operator, for Client-side connections are provided by the Client.

1.9.5 Connection to ports on the Operator's equipment is made:

- Using 10GBASE-SR with duplex multimode fiber optic cables with LC-LC connectors and 10GBASE-SR modules;
- Using 1000BASE-LX with duplex multimode fiber optic cables with LC-LC connectors and 1000BASELX/LH modules;
- Using 1000BASE-T/1000BASE-TX with copper UTP Cat5e/Cat6 cables with RJ45 connectors.

1.9.6 The Client may use network interfaces with LC-LC connectors for duplex multimode fiber optic cables, with RJ45 connectors for UTP copper cables, with SFP+ connectors or QSFP connectors with SFP module adaptors using 10GBASE-SR or 1000BASE-LX/LH modules for multimode fiber optic cables and 1000BASE-T for UTP copper cables.

1.9.7 Bandwidth and duplex port mode on the Client equipment should be set to "auto".

1.9.8 For connection the Client must use PTP domain IDs provided by the Operator. Peering IP addressing, dynamic or static routing are not used.

1.9.9 The Operator sends PTP multicast traffic of one independent PTP domains on each connection

port.

1.9.10 Client network equipment facing the Operator equipment should have LLDP protocol enabled (if supported).

1.10 Equipment connection to the Operator equipment in Production, Game and UAT systems access segment for network traffic mirroring.

1.10.1 Client equipment is connected to the Production, Game and UAT systems access segment for network traffic mirroring through the Operator's equipment with 1 Gbit/s or 10 Gbit/s ports depending on mirrored ports.

1.10.2 Client equipment connection to the Operator is done by pair of ports (two ports for each connection) or one port for each connection, depending on the scheme of the mirrored connection.

1.10.3 Client equipment is connected to the Operator with the cables supplied by the Operator. Interim equipment and cables from Clients are not allowed.

1.10.4 SFP modules (if needed) for Operator-side connections are provided by the Operator, for Client-side connections are provided by the Client.

1.10.5 Connections to 10 Gbit/s ports on the Operator equipment are done in accordance with 10GBASE-SR standard with duplex multimode fiber cables with LC-LC connectors and 10GBASE-SR modules. The Client at its premises may use 10GBASE-SR modules on network interfaces with SFP+ ports or QSFP ports with SFP+ adapter modules.

1.10.6 Connections to 1 Gbit/s ports on the Operator's equipment are done in accordance with 1000BASE-T/1000BASE-TX standard with copper UTP Cat5e/Cat6 cables with RJ45 connectors. The client can also use network interfaces with RJ45 or SFP standard connectors using 1000BASE-T standard modules.

1.10.7 Bandwidth and duplex port mode on the Client equipment should be set to "auto".

1.10.8 Peering IP addressing, dynamic or static routing are not used.

1.10.9 On each connection port the Operator transmits mirrored traffic from single port of mirrored connection.

1.10.10 Client network equipment facing the Operator equipment should have LLDP protocol enabled (if supported).

1.11 VPN (Virtual Private Network) connection to the Operator equipment over the Internet.

1.11.1 Secure access to the Operator's Production and Game systems access segment is performed over the Client's Internet connection provided by the telematics service operator as chosen by the Client.

1.11.2 Recommended Internet connection bandwidth is 4 Mbit/s per gateway/terminal used.

1.11.3 For establishing the connection Client must use settings provided by the Operator: the domain name or IP address of the VPN gateway and account details.

1.11.4 To enable connection to Moscow Exchange services, the Operator reserves specific IP addresses for the Client using the RFC 1918 space.

1.12 Cabling works

1.12.1 Any cross-connect works, incl. connecting, moving or disconnecting, on any Operator equipment, including patch panels are done only by the Operator representatives.

1.13 Timing of works

1.13.1 The following time interval names are set:

- Business hours — 8:00-24:00 on business days;

- Non-business hours — 0:00-8:00 on business days, around the clock on other days;
- Maintenance hours — 10:00-18:00 at weekends and public holidays.

1.13.2 The Client must setup and make changes to the network configuration of the equipment in the Operator networks in non-business hours.

1.13.3 Further time limitations may apply due to the following reasons:

- The Exchange opens markets on a non-business day (the trading day is deemed to a business day);
- The Exchange runs release, load or other testing (the testing day is deemed to be a business day);
- A release of the MOEX trading platform is expected as well as wide-scale works in the MOEX network, Colocation Facility, Operator's equipment or infrastructure; in this case, Moscow Exchange reserves the right to apply moratorium on any changes in the Operator's networks for the day of the event and several days prior to the event;
- Public holidays;
- Any other reasons upon additional notification from colo@moex.com.

1.14 Planning and coordination of setup and changes in the Client network equipment configuration

1.14.1 Setup and changes in configuration of the Client network equipment connected to the Operator network segments that may potentially affect the Operator network functionality should be approved by the Operator.

1.14.2 In order to approve the time and scope of such maintenance, the Client should submit a request and obtain approval from the Operator network specialists beforehand (at least 1 business day before the planned maintenance).

1.14.3 Depending on scope and complexity of works, the Operator reserves the right to request detailed documented plans of changes, to the point of specifying particular network equipment or individual ports configuration as well as postponing the maintenance to more suitable time interval.

1.14.4 If necessary (in the Operator's opinion), the Client must contact and keep in touch with the Operator representatives in order to mutually coordinate the maintenance process.

1.14.5 Changes in client equipment configuration should be completed in reasonable time before the markets open so that the Operator specialists could confirm that Moscow Exchange network performance is not affected.

1.15 Service request procedure

1.15.1 In order to submit the service request, the Client should contact the Operator using technical support public contacts.

1.15.2 Every unit of the Client equipment delivered to the Colocation Facility is given a unique ID (the "MOEX-ID"). Labels with MOEX-IDs are put on three sides of the equipment (upper, front and back panels) to ensure unambiguous identification of the equipment inside the rack.

1.15.3 When ordering services that require physical access of the Operator representatives to the Client equipment, the Client must specify MOEX-ID to avoid improper identification.

1.15.4 The following information may be required to perform certain maintenance works:

- Full name of the Client representative;
- Equipment name and labeling;
- Model and serial number;
- Number of interfaces and ports;
- Number of racks and units;
- IP addresses, numbers of IP protocols, number of TCP/UDP ports; traffic direction;

- IP addresses purposes;
- Other information.

1.15.5 In order to avoid any possible mistakes, such information should be provided via an e-mail.

1.15.6 In order to provide technical service or provide specific confidential information, the Client and/or its representative must be properly authorized.

1.15.7 Detailed description of authentication and authorization methods are described in paragraph 1.16 "Client authorization" of this document.

1.15.8 Sample forms of maintenance requests and authorization messages are given in the appendices to these Regulations:

- Appendix 1. Client authorization form
- Appendix 2. Operator connection request form
- Appendix 3. IP address request form
- Appendix 4. Firewall rules change request form for Internet access to equipment
- Appendix 5. Cross-connection removal request form

1.16 Client authorization

1.16.1 In order to request technical service, receive confidential information or material assets (equipment) as well as access equipment to perform planned or emergency maintenance, client representatives should be authorized.

1.16.2 Client's and its reps' personal Data used for authentication, as well as the powers of attorney of the Client representatives are specified in the Client Authorization form (in the form of power of attorney), as specified in Appendix 1 to the present Rules and Conditions which should be signed by authorized Client representative in accordance with the law and the company constituent documents. The Client Authorization Form is provided to the Operator.

1.16.3 The Client Authorization Form is deemed accepted by the Operator for use in client authentication and his trustees upon receipt of the signed copy.

1.16.4 Client Authorization Forms are assigned unique numbers and can be executed at any time during the contract term, in this case, once the new Client Authorization Form version is signed, the previous Client Authorization Form becomes void.

1.16.5 The Operator accepts the following authorization methods:

- Requests received from the email address specified in the colocation agreement as primary contact email address;
- Requests from the person authorized by the Client acting in accordance with the Client Authorization Form (in power of attorney form) stated in Appendix 1 of the present Rules and Conditions - for actions to which the representative has been authorized by the Client.

1.16.6 In case of the authorized person's dismissal or appointment of a new authorized person by the Client, as well as in case of any change of Client information stated in the Client Authorization form, the Client is obliged immediately to inform the Operator by contacting technical support and then submit an updated Client Authorization Form to the Operator within three (3) calendar days.

1.16.7 The Operator interacts with the Client on the following questions:

- Organizational matters;
- Technical questions/issues, requests for technical service.

Appendix 1. Client Authorization Form

Client Authorization Form No. ____
(power of attorney form)

Moscow

Client	
Technical Center	Moscow Exchange
Operator	MOEX Information Security
Agreement with the Technical Center	No. _____ dated ____ _____20_
Agreement with the Operator	No. _____ dated ____ _____20_

1. Client emergency contact details

Email address for emergency text messages	

2. Power of attorney

By signing this form the Client authorizes the following person(-s) to perform the following actions on behalf of the Client:

Full name		
Passport number and validity dates		
Email		
Telephone number		
Scope of actions	Moscow Exchange	MOEX Information Security
Communication with the Technical Center/ Operator regarding the organizational matters with the right to sign the service/service change requests, termination notices re the agreement, other documents set out in the Rules and Regulations	☐	☐
Communication with the Technical Center/Operator regarding technical matters with the right to submit requests to fix service issues	☐	☐
DC visit requests	☐	
Bringing the Client equipment into the DC	☐	
Physical access to the equipment	☐	
Taking the equipment out of the DC	☐	

(to be completed individually for every person)

3. Period of validity

This Client Authorization Form (power of attorney) is valid for 3 (three) years since the date of signature.

On the date of this Authorization Form signature, the previous Authorization Form #____ dated _____ 20_, including its power of attorney is revoked and becomes void.

In witness thereof, this Client Authorization Form is signed by the authorized representative of the Client (the head of the legal entity or any other person duly authorized to do so in accordance with the law and the company's constituent documents)*.

By the Client:

_____
Signed Full name

_____ 20_

***** *If the signatory is acting on the basis of the power of attorney* ***with the right of substitution****, the following documents shall also be submitted:*
• the original or a notarized copy of the power of attorney confirming the powers of the person to sign the form;
• the document confirming the powers of the person who issued the power of attorney or the notarized copy thereof, or the extract therefrom certified with the signature of the authorized person and the seal (if any).

Appendix 2. Sample request for connection to the Operator's equipment

Request for connection to the Operator's equipment

Please connect to the Operator's equipment under agreement No _____/CLZ dated _____20___.

Connection parameters:

Segment: Productions and Game; UAT network, Internet

Connection type (L2/L3): _____

Equipment label: _____

Port name/number: _____

Title
Full name
Contact details

Note: *please submit this request to colo@moex.com by using the authorized email address.*

Appendix 3. IP allocation request

IP allocation request

We request the following IP addresses to the allocated within the Internet-Facing Network Segment in accordance with the agreement No.____/CLZ dated __ _____ 20__:

Internet access:

Internet access for mgmt interface:

Title
Full name
Contact details

Note: *please submit this request to colo@moex.com from authorized Email address.*

Appendix 4. Firewall rules change request form

Firewall rules change request

In accordance with colocation agreement №____/CLZ as of __ _____ 20_ please make changes into the firewall rules for inbound/outbound (select appropriate) internet access as follows:

Add permissions:

Inbound/outbound traffic	IP address(es) in private network	Internet IP address(es)	List of protocols/ports

Remove existing permissions:

Inbound/outbound traffic	IP address(es) in private network	Internet IP address(es)	List of protocols/ports

Title
Full name
Contact details

Note: *please submit this request to colo@moex.com from authorized Email address.*

Appendix 5. Sample request for cross-connection removal

(to be completed by the **Client initiated the cross-connection**)

Cross-connection removal request

Please remove the connection to the Operator equipment under agreement No _____/CLZ dated _____20___.

Connection parameters:

Segment: Production and Game; UAT, Internet

Connection type (L2/L3): _____

Equipment label: _____

Port name/number: _____

Title
Full name
Contact details

Note: *please submit this request to colo@moex.com by using the authorized email address.*