THE NIX.CZ ASSOCIATION
INTERNAL RULES AND REGULATIONS

(Version 11 dated 2022/06/19 effective from 2023/01/01)

Article I
NIX.CZ ASSOCIATION MEMBERSHIP PREREQUISITES

1.1 Any legal entity applying for membership in the NIX.CZ Association must meet the following criteria:

a) The entity has been assigned its own Autonomous System Number (ASN). In the event that the legal entity applying for membership in the Association has not been assigned its own ASN, a written consent of the ASN owner must be provided.

Article II
PREREQUISITES FOR CONCLUDING A CUSTOMER CONTRACT WITH THE ASSOCIATION

2.1 Any legal entity requesting to enter into a customer contract with the NIX.CZ Association must meet the following criteria:

a) The entity has been assigned its own Autonomous System Number (ASN).
b) In case the legal entity requesting to enter into a customer contract with the Association has not been assigned its own ASN, a written consent of the ASN owner or proof of provision IPTV or VoD services must be provided
c) The entity undertakes to comply with the terms and conditions stated in the Association´s Internal Rules and Regulations and in the Association´s Price List.

Article III
OPERATING CONDITIONS

3.1 Connection to NIX.CZ nodes will be allowed after the initial membership fee has been paid according to the statutes of the association (member of the Association) or a service contract has been signed (customer of the Association).

3.2 Each member/customer shall cooperate with an authorized employee of the NIX.CZ Association (hereinafter referred to as the "**association engineer**") during the set-up of a connection to the NIX.CZ nodes and during its maintenance.

3.3 Before connecting to the NIX.CZ infrastructure, each member/customer is obliged to provide and keep up-to-date the following information on the Extranet:

a) operation contact details, including:
   i) A telephone number available 24 hours a day, 7 days a week
   ii) An e-mail address of their NOC (Network Operation Center);

b) e-mail addresses to be listed on the NIX.CZ contact list for the purposes of correspondence between members/customers;

c) Autonomous System Number (ASN) assigned to the relevant Member/Customer;

d) the full canonical name for member´s/customer´s router which will be registered in the reverse domains (in-addr.arpa a ip6.arpa) within the domain name system assigned to the NIX.CZ Association;

e) the URL of the member´s/customer´s website, if the member/customer requires a link from the Association´s website;

f) e-mail address for peering requests;

g) contact information of the member/customer

3.5 In case the stability and functionality of NIX.CZ equipment is jeopardized by an equipment/connection belonging to a member/customer, the Association shall be entitled to block the relevant member´s/customer´s port until the problem has been resolved by the member/customer. Employees of the Association will, in such case, immediately inform the NOC contact (as registered on the Association´s extranet) by e-mail. This obligation to inform does not apply to the automatic port blocking pursuant to Item PI/13 Annex 1 hereof.

3.6 The technical operating conditions for public peering (VLAN) are specified in Annex I to these Internal Rules and Regulations. The technical operating conditions for the private VLAN are specified in Annex II to these Internal Rules and Regulations. The technical operating conditions for the multicast segment (VLAN) are specified in Annex III to these Internal Rules and Regulations.

Article IV
OTHER CONDITIONS OF USE

4.1 Members/customers must ensure that their connection to the NIX.CZ node did not cause harm to the use of NIX.CZ services by other members/customers.

4.2 Members/customers must not use NIX.CZ to carry out any illegal activities.

4.3 The use of certain cyber-attack mitigation techniques by the Association in accordance with the documentation published on the Association´s extranet is not considered a violation of these Internal Rules and Regulations.

Article V
INSURANCE AND LIABILITY

5.1 In the event of any claims for damage caused by any member/customer of the Association to another member/customer of the Association or directly to the Association, the procedure will take place in accordance with the applicable legislation.

Annexes:

Annex I	– Technical Operating Conditions for public peering segment (VLAN)
Annex II	– Technical Operating Conditions for private VLAN
Annex III	**– Technical Operating Conditions for multicast peering**

Annex I

TECHNICAL OPERATING CONDITIONS FOR PUBLIC PEERING SEGMENT (VLAN)

PI/1. The common network technology of the NIX.CZ node is Ethernet (IEEE 802.3)

PI/2. NIX.CZ offers the following interfaces:

a) 1Gb/s optical port with 1000BASE-LX module;
b) 10Gb/s optical port 10GBASE-SR or 10GBASE-LR module;
c) 100Gb/s optical port with 100GBASE-SR10 or 100GBASE – LR4 module;
d) 400Gb/s optical port with 400GBASE-FR4 or 400GBASE-LR4 module;
e) In case of a request for another module that has not been mentioned previously, the procedure will be based on the agreement with the Association´s engineers (in particular ER, ZR, xWDM modules etc.);

PI/3. Members/customers are entitled to use the public peering segment of NIX.CZ for internal transit of their networks

PI/4. Multiple physical ports of the same member/customer terminating in the same NIX.CZ switch can be grouped into a single logical port (EtherChannel). Such connection of ports is configured using LACP (Slow LACPDUs)

PI/5. Each member/customer connection to the peering segment is limited to 1 source MAC address

PI/6. Ethernet frames sent by a connected device to a shared segment must have one of the following ethertypes:

a) 0x0800 – IPv4;
b) 0x0806 – ARP;
c) 0x86dd – IPv6;

PI/7. Frames forwarded to the shared segment must not be addressed to a multicast or broadcast MAC with the following exceptions:

a) ARP broadcast;
b) IPv6 neighbor discovery;
c) Others, if necessary, based on a permission by the Association

PI/8. Broadcast and multicast frames sent to the peering segment are rate-limited

PI/9. Any of the local-link protocols (see PI/10) cannot be forwarded to the peering segment with the exception of:

a) ARP (not Proxy-ARP);
b) IPv6 neighbor discovery.

PI/10. Link-local protocols are (not limited to): IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protocols such as (CDP etc.), interior routing protocols (OSPF, ISIS, EIGRP), BOOTP/DHCP, PIM-SM/PIM-DM, DMVRP, Mikrotik Neighbor Discovery Protocol (MNDP), IPv6 RA etc.

PI/11. Traffic generated by APR/ND protocols cannot exceed 50 packets/s for each.

PI/12. ASBR router port connected to the peering segment must have the proxy-arp feature disabled. NIX.CZ performs periodic checks on settings in the peering segment.

PI/13. Newly installed ports are placed in the isolated quarantine environment, where all customer's port configuration checks are performed. Moving the customer's port into production peering VLAN is only possible after all misconfiguration is fixed.

PI/14. In case of exceeding a maximum number of MAC addresses on the port, or in case of PI/9 violation, the peering port can be disabled to keep the peering segment secured.

PI/15. All ports connected to the peering segment must use the IP address and mask assigned by NIX.CZ technicians. For each physical/logical port, one IPv4 and one IPv6 address are assigned.

PI/16. IPv6 addresses must be configured statically (no automatic configuration). IPv6 site-local IP addresses cannot be used.

PI/17. IP packets with the peering segment broadcast address cannot be sent to the member/customer's port.

PI/18. The routing protocol of NIX.CZ nodes is BGP-4 (RFC-4271) with possible extension to MP-BPG-4 (RFC4760, RFC-2545) – only unicast IPv4 and IPv6.

PI/19. Addresses of the common network segment shall not be advertised to other networks without explicit permission of NIX.CZ Association.

PI/20. Traffic from the port of one member/customer can be forwarded to the address of another member/customer only upon peering agreement and only via BGP-4 protocol (see PI/17).

PI/21. All routes advertised across the common network segment shall point to the router advertising them, with the sole exception of deploying the RTBH filtering function (see PI/21) or based on a prior agreement made in writing by NIX.CZ and all members/customers involved.

PI/22. Customer's / Member's port cannot be loaded more than 90% in 5 minutes intervals.

PI/23. All members/customers are requested to follow the recommendations below:

a) Recommended **peering policy**:

1) register their routing policy for each connected ASN in the RIPE database and keep it updated;
2) for all networks advertised via BGP register a route (or route6) object in the RIPE database or similar register and keep it updated;
3) use an as-set object registered in RIPE database or similar register
4) register company's record in PeeringDB and keep it updated
5) to monitor advertised prefixes states using own tools

b) Recommended **peering router** configuration:

1) using Control Plane Policing (CoPP) preventing DDoS on peering router
2) using a traffic monitoring and other security tools analyzing security breach
3) using mitigation tools against (D)SoS and other security attacks, like RTBH, IPS etc…
4) using a BCP-38 for own peering router

c) Recommended **peering port** configuration:

1) Disable ICMP and ICMPv6 redirect messages.
2) Disable ICMP and ICMPv6 unreachable messages.
3) Disable IPv6 Multicast Listener Discovery protocol.
4) Suppress IPv6 Router Advertisement transmission.
5) Use IPv6 ND cache limitation.
6) Use min. BFD interval 1000ms with 5 as a multiplicator.
7) Disable services not in use, such as NTP etc.
8) Use the MTU settings as 1500-byte

d) Recommended **BGP peering** configuration:

1) Do not generate useless "route flaps".
2) Do not advertise more specific routes without a reason.
3) Use a limit of max. no. of 64 for BGP community attribute.
4) Use a limit of max. no. of 64 for BGP ext- and large-community attribute.
5) Use a limit of max. ASNs in the BGP patch attribute.
6) Use a maximum prefix count on each IPv4 and IPv6 BGP session with automatic recovery.
7) Use IPv4 and IPv6 prefix aggregation function in the database.
8) Use BFD fall-over protocol for IPv4 and IPv6 peers.
9) Use authentication mechanism (MD5) for TCP connection with IPv4 a IPv6 peers.
10) Use Generalized TTL Security Mechanism check with IPv4 and IPv6 BGP peers.
11) Sign all advertised prefixes using RPKI ROA.
12) Prefer RPKI valid over RPKI unknown/RPKI invalid

e) BGP configuration with Route Servers

1) Accepted prefix length maximum is /24 for IPv4 and /48 for IPv6
2) Bogon and martian prefixes are not accepted
3) AS-PATH cannot be longer than 64 ASNs and AS-PATH aggregation is not supported. We force BCP172/RFC6472 compliance.
4) Peering BGP ASN has to be equal with first ASN in the AS-PATH of the advertised prefix.
5) Prefix’s next-hop IP address attribute in a BGP must match with BGP session IP address.
6) IP prefix cannot contain “Tier 1” ASN in AS-PATH
7) Origin ASN of the advertised prefix must be included in AS-SET of the BGP peer.
8) Route servers are configured with RPKI ROV, RPKI invalid prefixes are not allowed and are filtered.
9) Prefix is compared with IRRDB (radb.net) and it is only allowed when correct “route-object” is defined within allowed ASN list.

Annex II

TECHNICAL OPERATING CONDITIONS FOR PRIVATE SEGMENT (VLAN)

PII/1. Physical connection is specified in PI/1 – PI/2 and PI/4

PII/2. Each customer's/member's private VLAN is limited to 2 source dynamic MAC addresses.

PII/3. Broadcast and multicast frames sent to the peering segment are rate limited.

PII/4. Layer 2 frames sent to the peering segment cannot be: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protocols (CDP etc.), IGMP, PIM-SM/PIM-DM, DMVRP etc.

PII/5. ARP/ND packets generated to the peering segment cannot exceed 20 packet per second.

PII/6. Newly installed ports are placed in the isolated quarantine environment, where all customer's port configuration checks are performed. Moving the customer's port into production peering VLAN is only possible after all misconfiguration is fixed.

PII/7. In case of exceeding a maximum number of MAC addresses on the port, or in case of PI/9 violation, the peering port can be disabled to keep the peering segment secured.

PII/8. Customer's / Member's port cannot be loaded more than 90% in 5 minutes intervals.

PII/9. We do recommend:

a) To realize direct connection to ASBR, not using intermediate L2 device.

b) Private VLAN can be used to transport internal routing protocols like OSPF, ISIS, EIGRP, iBGP, BOOTP/DHCP, IPv6 router advertisement and others.

PII/10. On ports using multicast VLAN services, the MTU switch settings can be increased, provided the responsible employees of the Association give a written agreement, to 9216B. Members/customers must comply with the size of the MTU in the peering segment in accordance with PI/23.c)

Annex III

TECHNICAL OPERATING CONDITIONS FOR A MULTICAST SEGMENT (VLAN)

PIII/1. Physical connection is specified in PI/1 – PI/2 and PI/4

PIII/2. Broadcast and multicast frames sent to the peering segment are rate limited.

PIII/3. Layer 2 frames sent to the peering segment cannot be: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protocols (CDP etc.), IGMP, PIM-SM/PIM-DM, DMVRP etc.

PIII/4. ARP/ND packets generated to the peering segment cannot exceed 20 packet per second.

PIII/5. Newly installed ports are placed in the isolated quarantine environment, where all customer's port configuration checks are performed. Moving the customer's port into production peering VLAN is only possible after all misconfiguration is fixed.

PIII/6. In case of exceeding a maximum number of MAC addresses on the port, or in case of PI/9 violation, the peering port can be disabled to keep the peering segment secured.

PIII/7. Customer's / Member's port cannot be loaded more than 90% in 5 minutes intervals.

PIII/8. Multicast segment (VLAN) topology is point-to-point.(source - destination).

PIII/9. Members/customers shall comply with the addressing of the multicast traffic determined by the IANA, i.e. class D group - 224.0.0.0/4

PIII/10. Members/customers are recommended to:

a) Apply direct connection to their own edge router without further L2 equipment.

b) Not use overlapping multicast addresses in mapping multicast IP onto MAC addresses 32:1.

Examples of overlapping addresses::

224.1.1.1
224.129.1.1
225.1.1.1
225.129.1.1
.
.
.
238.1.1.1
238.129.1.1
239.1.1.1
239.129.1.1

c) Multicast VLAN can be used to distribute IPTV, VoD etc.

PIII/11. On ports using multicast VLAN services, the MTU switch settings can be increased, provided the responsible employees of the Association give a written agreement, to 9216B. Members/customers must comply with the size of the MTU in the peering segment in accordance with PI/23.c)