Namex Technical Regulations

Version: 1.0
Publication Date: 23 September 2026
Approved by the Namex Board of Directors

Indice

1 Introduction

These Technical Regulations define the technical specifications, requirements, and operational rules applicable to entities accessing and utilizing the interconnection infrastructure and services provided by Namex (hereinafter referred to as "Participants").

The provisions set forth in this document are intended to ensure a neutral, open, secure, stable, and efficient interconnection environment for the benefit of all Participants and the broader Internet ecosystem.

Compliance with these Regulations is a mandatory condition for accessing and maintaining the services provided by Namex.

1.1 Scope and Applicability

These Technical Regulations apply to all Participants and govern access to, connection with, configuration, and use of the interconnection infrastructure and services provided by Namex.

The provisions set forth in this document apply to all physical and logical infrastructure managed by Namex, including interconnection platforms, peering services, support systems, and any other technical service that may be provided.

These Regulations supplement and form an integral part of the contractual terms and other applicable documents for Namex services. Participants are required to comply with its provisions throughout the duration of their contractual relationship with Namex.

Participants are also responsible for ensuring compliance with these Regulations by their personnel, vendors, and any authorized party operating on Namex infrastructure on their behalf.

Namex reserves the right to update these Technical Regulations to adapt them to technological evolution, industry best practices, and the operational requirements of the infrastructure. Any modifications will be communicated to Participants through appropriate channels and with adequate notice.

2 Admission Rules

2.1 Legally recognized entities, such as network operators, Internet service providers, content providers, cloud providers, carriers, public bodies, and other entities engaging in activities consistent with the interconnection purposes of the Internet Exchange, are eligible for admission to Namex services.

2.2 Applicants must meet the following requirements:

- 2.2.1 Ensure to Namex that they possess the necessary legal authority and ownership of the resources and infrastructure used, as well as the capacity to comply with all provisions of these Technical Regulations.
- 2.2.2 Hold or be an authorized user of at least one public Autonomous System Number (ASN) and public IP addresses assigned by a recognized Regional Internet Registry (RIR).
- 2.2.3 Maintain public IP connectivity and possess the technical capacity required to manage peering sessions via the BGP protocol.
- 2.2.4 Provide Namex with the requested documentation to verify compliance with the necessary technical and administrative requirements.
- 2.2.5 Commit to complying with the technical, operational, and security rules defined by Namex for the use of its infrastructure and services.

2.3 Applications for admission are evaluated by the Technical Committee, which issues an opinion regarding compliance with the specified requirements. Admission is approved by the President of the Consortium, after consulting the Technical Committee, and is subject to ratification by the Board of Directors.

3 General Rules

3.1 All costs associated with the implementation and maintenance of connections between the Participant's infrastructure and the Namex exchange points are to be borne entirely by the Participant.

3.2 Participants' activities at Namex must comply with applicable laws and regulations, and must not in any way infringe upon any laws, regulations, or third-party rights.

3.3 Participants are responsible for the traffic generated and exchanged through Namex infrastructure and undertake to use the services strictly for lawful purposes consistent with the objectives of Internet interconnection and traffic exchange.

3.4 Participants must communicate and keep their operational and administrative contact details up to date, providing at least the following contacts:

3.4.1 A technical contact responsible for receiving communications regarding technical configurations, service activations and modifications, scheduled maintenance, troubleshooting, and technical compliance verifications, available at least during standard business hours.

3.4.2 An operational contact (NOC), available 24 hours a day, 7 days a week, responsible for receiving communications regarding incidents, operational emergencies, network anomalies, and events requiring prompt intervention or immediate coordination.

3.4.3 An administrative contact responsible for receiving communications regarding contractual, administrative, documentation, and billing matters.

3.4.4 An official contact, designated for formal communications of institutional representation, including assembly notices, event invitations, ceremonies, official Consortium communications, and escalation procedures should issues remain unresolved through the contacts listed above.

3.4.5 Additional specific contacts, such as peering, security, or billing representatives, or other operational roles, may be requested by Namex in accordance with the procedures set out in the admission form and operational documentation.

3.5 For each contact, the name, role, email address, and telephone number must be provided. Participants are required to ensure their availability in accordance with the declared functions and the availability levels required by these Regulations.

3.6 Participants are required to communicate any changes to the provided contact details, ensuring that the information remains updated throughout the entire duration of their relationship with Namex.

3.7 The email addresses provided pursuant to this section may also consist of group addresses or distribution lists, provided they effectively guarantee receipt of communications by the competent personnel for the declared function. The Participant remains fully responsible for ensuring the proper operation and updating of such email addresses.

3.8 Equipment owned by the Participant and housed at Namex premises must be covered by an adequate insurance policy against theft, fire, and third-party liability. The Participant remains liable for any damage caused to Namex infrastructure or to third parties.

4 Technical Rules Regarding Colocation Services

4.1 General Rules for Colocation Services

4.1.1 Site-specific technical, operational, logistical, and security requirements may apply to each location, as well as specific procedures for access, installation, cabling, power supply, and infrastructure management, as detailed in the Appendices and technical documentation referenced in Article 4.5.

4.1.2 All equipment and systems housed at Namex premises must comply with the technical and environmental requirements established by the host data center, including, but not limited to, parameters regarding temperature, humidity, power supply, heat dissipation, and overheat protection.

4.1.3 Participants are responsible for the proper installation, configuration, and management of their equipment, as well as for implementing adequate security measures to ensure the stability and integrity of the Namex infrastructure and the data center.

4.1.4 Equipment must be installed and cabled in compliance with the operational procedures and technical instructions provided by Namex and the host data center. Modifications that could interfere with shared infrastructure or the equipment of other Participants are strictly prohibited.

4.1.5 Physical access to colocation areas is restricted exclusively to authorized data center personnel, Namex, and personnel designated by the Participant, in accordance with applicable security procedures. All access must be authorized in advance and tracked.

4.1.6 The host data center and Namex reserve the right to schedule routine and extraordinary maintenance work on the infrastructure. Participants will be notified in advance, except in cases of emergency.

4.1.7 In emergency situations or where safety and security risks are present, data center or Namex personnel may perform interventions on the housed equipment without prior authorization from the Participant, strictly limited to what is necessary to ensure operational continuity and infrastructure security.

4.1.8 Upon termination of the colocation contract or in the event of service discontinuation, the Participant is required to remove their equipment and materials within the timeframe specified by Namex. In the event of non-compliance, Namex reserves the right to proceed with the removal in accordance with the procedures set forth in the contractual terms and conditions.

4.1.9 Installed equipment must comply with the power limits and power supply requirements established by the data center and communicated by Namex (see Article 4.5 regarding site-specific requirements). The Participant is responsible for proper power sizing and for the implementation of redundant power systems, where required.

4.1.10 All devices, rack units, and connections must be clearly identified with labeling in order to enable efficient and secure management of the infrastructure.

4.1.11 Cabling must be executed in accordance with the technical standards defined by Namex and the data center, using certified materials and maintaining an adequate level of order and safety within the assigned spaces.

4.1.12 The installation or use of unauthorized equipment, or equipment that could compromise the physical or logical security of the infrastructure, is strictly prohibited, as is the introduction of devices that may interfere with the activities of other Participants.

4.2 Installation Requirements

4.2.1 Housed equipment and systems must be rack-mountable for installation in standard 19" racks and powered by 220 Volt AC, unless different technical specifications are communicated by Namex or the data center.

4.2.2 Equipment must be installed exclusively within the assigned spaces and in accordance with the instructions provided by Namex or host data center technical personnel.

4.2.3 Equipment dimensions must not exceed the depth of the assigned rack or prevent the proper closing of the cabinet's front or rear doors.

4.2.4 All housed equipment and systems must be clearly identifiable by means of appropriate labeling that includes at least the Participant's name and the necessary information for operational management.

4.2.5 Cabling within racks and cabinets must be executed in a neat and structured manner to ensure proper airflow, safety, and ease of maintenance. Namex reserves the right to request the reorganization of cabling if it fails to comply with the defined standards.

4.2.6 The installation of Participant-owned Power Distribution Units (PDUs) is prohibited, unless explicitly authorized by Namex and the data center.

4.2.7 The installation of energy storage systems or batteries within colocation areas is prohibited without prior formal authorization from Namex and the host data center. Where authorized, the Participant must comply with all applicable safety, installation, management, and maintenance standards. Batteries must be maintained in according with manufacturer specifications and subjected to documented periodic inspections to ensure proper operation and infrastructure safety.

4.2.8 Where technically feasible, equipment must be equipped with redundant power supplies and connected to separate power feed lines, in compliance with the technical instructions provided by the data center and Namex.

4.2.9 The Participant is responsible for accurately sizing the energy consumption of their equipment and must communicate both nominal and maximum power absorption values to Namex. Namex reserves the right to verify these values and to request adjustments should the allowed thresholds be exceeded.

4.2.10 It is prohibited to introduce or use materials, devices, or configurations that could compromise fire safety, ventilation, or the environmental conditions of the data center. All materials used must comply with applicable safety standards.

4.2.11 Equipment must be installed using suitable mounting hardware and, where necessary, other technical components designed to ensure proper airflow management and energy efficiency, in compliance with the instructions provided by Namex or the host data center.

4.3 Power Supply Requirements

4.3.1 Participants undertake to inform Namex technical personnel, at the time of installation, of the expected power consumption for each piece of equipment, as well as the total combined power consumption of all installed active equipment.

4.3.2 Participants undertake to inform technical personnel of any variation in previously declared power consumption values, particularly in the event of equipment replacement, upgrade, or reconfiguration.

4.3.3 Power consumption is subject to periodic verification by Namex or the data center to ensure compliance with declared values and adherence to applicable technical and contractual limits.

4.3.4 Should power consumption be found to exceed declared values or fail to comply with applicable limits, Namex reserves the right to require the Participant to take necessary corrective actions, including the reconfiguration, replacement, or removal of the equipment, as well as the potential adjustment of contractual terms.

4.3.5 In the event of situations that may compromise the security or stability of the electrical infrastructure, Namex and the data center reserve the right to take urgent measures—including cutting off the power supply to the affected equipment—and will inform the Participant accordingly.

4.4 Backbone Connections and External Access Points

4.4.1 All fiber optic connections originating from the outside must terminate exclusively at the manholes or entry points designated by the data center and communicated by Namex. These access points must be used in compliance with the established operational and security procedures.

4.4.2 It is prohibited to establish unauthorized connections or attempt to access any area of the data center other than the explicitly authorized entry points.

4.4.3 The Participant, or any appointed third-party vendors, must request and obtain prior authorization from the data center and Namex before performing any installation, maintenance, or modification activities on fiber optic connections.

4.4.4 The internal cable routing must be agreed upon and approved by the data center and Namex technical personnel prior to installation.

4.4.5 It is mandatory to use existing containment infrastructure, such as conduits, cable trays, or dedicated overhead systems. The installation of new cabling infrastructure is permitted exclusively upon formal approval from the data center and Namex.

4.4.6 All cables must be installed in an orderly manner to minimize the risk of accidental damage, interference, and service disruptions. Cables must be labeled both at the data center entry point and at the internal termination points.

4.4.7 Participants are responsible for the management, maintenance, and integrity of their own connections, as well as for any damage caused to the infrastructure or to other Participants.

4.4.8 Namex and the data center reserve the right to request the removal, modification, or securing of any connections that do not comply with technical standards or operational procedures.

4.4.9 Participants are encouraged, where possible, to implement physically diverse routes for their connections in order to enhance resilience and service continuity.

4.4.10 Connections must use fiber types, connectors, and termination methods that comply with the technical standards specified by Namex and the host data center. Any specific requirements regarding single-mode, multi-mode, optical connectors, and transmission standards will be communicated in the applicable technical specifications.

4.5 Site-Specific Requirements

4.5.1 The technical, operational, and security requirements specific to each data center or Namex site are detailed in the Appendices to this Technical Regulation, entitled "Site-Specific Requirements for Data Centers".

4.5.2 These documents form an integral part of this Regulation and define the operational procedures, access protocols, technical requirements, and any additional provisions applicable to the infrastructure and services provided at each site.

4.5.3 The single interference risk assessment documents (DUVRI) and the emergency and evacuation plan (PEE) applicable to individual sites constitute complementary documentation to the requirements of this article and are available for consultation at the Namex operational headquarters.

4.5.4 Participants are required to know and comply with the requirements applicable to the site or sites where their infrastructure is present.

4.5.5 Namex reserves the right to update the Appendices in order to adapt them to technological developments, operational needs, and industry best practices. Any modifications will be communicated to Participants through appropriate channels and with adequate notice.

5 Technical Rules for Connecting to Service Delivery Platforms

The provision of Namex services is subject to the Participant connecting to one or more interconnection platforms, in accordance with the technical and operational procedures set forth in this section.

5.1 Passive Interconnection Platforms

5.1.1 A passive interconnection platform enables the establishment of physical point-to-point fiber optic connections within a specific site (data center).

5.1.2 The passive interconnection platform consists of one or more meet-me room termination frames, interconnected via structured cabling provided by Namex or the facility operator.

5.1.3 The Participant's connection to the passive interconnection platform is established by installing a structured single-mode fiber optic trunk between the assigned colocation space and the nearest meet-me room termination frame.

5.1.4 The connection is terminated at both ends by presentation patch panels equipped with LC/PC duplex connectors, appropriately cataloged and labeled.

5.1.5 The identification of the patch panel must include information regarding the source and destination of the optical connection, including:

5.1.5.1 host rack name,

5.1.5.2 rack unit number,

5.1.5.3 applicable module or position within the rack unit.

5.1.6 The installation of the optical connection is performed by Namex or, where applicable, by the host facility operator, using technologies deemed suitable, without prejudice to the presentation standard described above.

5.1.7 The presentation patch panel installed within the Participant's rack space constitutes the demarcation point of responsibility for passive interconnection services.

5.2 Active Interconnection Platforms (Switching)

5.2.1 Active interconnection platforms enable the provision of public peering services as well as private interconnection services based on Ethernet technology.

5.2.2 These platforms consist of a set of switching devices operating at Layer 2 of the ISO/OSI model, interconnected to support one or more broadcast domains, appropriately segregated using VLANs.

5.2.3 The Participant's connection to the active interconnection platform is established by connecting to one or more physical ports of an access switch, using the infrastructure and procedures described in the section relating to the passive interconnection platform.

5.2.4 Connections are established using duplex optical interfaces (TX/RX) compliant with the standards set out in Appendix 1.

5.2.5 It is possible to aggregate multiple physical ports into a single logical interface in accordance with the IEEE 802.3ad standard, either in static mode or using the LACP protocol.

5.2.6 The Participant may have multiple connections to the active platform, for example to distribute traffic or ensure redundancy and resilience.

5.2.7 The total traffic carried by the Participant across its connections to the active platform is subject to monitoring for the purpose of assessing capacity usage. The measurement criteria and operational procedures are established by Namex and are detailed in Appendix 3 – Traffic Measurement Procedures.

5.3 Remote Aggregation Platforms (Reseller)

5.3.1 Remote aggregation platforms enable the transport and routing of data flows relating to remote customers, conveyed by a Participant acting as a reseller, towards the interconnection services provided by Namex.

5.3.2 These platforms consist of Layer 2 switching devices and use Ethernet technologies compliant with the applicable standards.

5.3.3 The Participant's connection to the remote aggregation platform is established by connecting to one or more physical ports of an access switch, using the infrastructure and procedures provided for interconnection platforms.

5.3.4 Connections are established using duplex optical interfaces (TX/RX) compliant with the standards set out in Appendix 1.

5.3.5 It is possible to aggregate multiple physical ports into a single logical interface in accordance with the IEEE 802.3ad standard, either in static mode or using the LACP protocol.

5.3.6 The Participant may have multiple connections to the remote platform, in order to distribute traffic and improve resilience.

5.3.7 Each connection to the remote aggregation platform may correspond to multiple logical connections to the other service delivery platforms.

5.3.8 Connections to the destination platforms are implemented and managed by Namex in terms of physical deployment, technologies used, and bandwidth capacity, based on the operational and contractual requirements of the remote customers.

5.3.9 The traffic carried by the Participant acting as a reseller — to and from the active interconnection platform only — is subject to monitoring for the purposes already set out in section 5.2.7 and according to the procedures described in Appendix 3 – Traffic Measurement Procedures, attributing the usage values of the individual connections to the active platform of the remote customers transported to the Participant's total count.

6 Technical Rules for Service Provisioning

6.1 In-Situ Physical Interconnection Services (PNI)

6.1.1 The physical interconnection service (PNI – Private Network Interconnect) consists of an optical connection established through the passive interconnection platform, connecting two terminal locations belonging to two distinct Participants.

6.1.2 A terminal location is identified by a port (fiber pair) on the presentation patch panel installed inside the Participant's rack.

6.1.3 The implementation of the optical path between the two terminal locations is carried out by Namex technical personnel by installing one or more patch cords within the passive interconnection platform.

6.1.4 Connections must be established using duplex optical patch cords (TX/RX), compliant with the applicable technical standards.

6.1.5 The physical interconnection service is identified by a unique code assigned by Namex upon completion of activation.

6.1.6 Upon completion of activation, Namex provides the interested Participants with the service identifier together with the technical documentation of the established optical path, indicating the individual segments and termination points.

6.1.7 Namex's scope of responsibility is limited to the segment between the two terminal locations of the respective Participants.

6.1.8 The connection between the Participant's network equipment and the terminal location on the patch panel is the responsibility of the Participant.

6.1.9 Each port (fiber pair) on the patch panel must correspond to one and only one physical interface of the Participant's network equipment.

6.1.10 Participants may not make direct connections between their own equipment or infrastructure using Namex resources without the explicit involvement and authorization of Namex.

6.1.11 Namex defines and communicates to the Participants the operational procedures and timelines for the activation, modification, and decommissioning of PNI services, as well as any scheduled maintenance windows.

6.1.12 Namex may carry out maintenance, verification, and reorganization work on the optical paths in order to guarantee operational continuity, security, and infrastructure optimization, giving prior notice to Participants except in emergency cases.

6.1.13 Participants are responsible for the proper configuration and management of their own equipment and transmitted optical power levels, as well as for the compatibility of the optical interfaces used.

6.1.14 In the event of performance degradation or anomalies on the connection, Participants shall collaborate with Namex in diagnostic and troubleshooting activities.

6.1.15 Any requests for expansion, upgrading, or implementation of redundant paths must be agreed upon with Namex in accordance with the applicable operational procedures.

6.2 Public Peering Service

6.2.1 The public peering service allows Participants, following the setup of one or more connections to the active interconnection platform, to access a distributed Layer 2 peering LAN, a dedicated IPv4 and IPv6 address space, and the support services necessary to establish bilateral and multilateral peering agreements for IP traffic exchange via the BGP protocol.

6.2.2 Participants may establish one or more connections to the active interconnection platform.

6.2.3 Each connection is assigned an IPv4 address and an IPv6 address within the subnets dedicated to the peering LAN.

6.2.4 Only one MAC address is permitted per connection, which must be associated with the assigned IP addresses.

6.2.5 Participants establish peering agreements using the BGP protocol and retain full autonomy in defining their peering policies, including the right to accept or reject peering requests.

6.2.6 Resale or transfer of the public peering service to third parties is not permitted, except with the explicit authorization of Namex.

6.2.7 Participants undertake to announce exclusively public IP prefixes associated with their own Autonomous System or those of their customers.

6.2.8 It is not permitted:

6.2.8.1 to announce default routes,

6.2.8.2 to provide global Internet access via the peering LAN,

6.2.8.3 to use tunneling, static routing, or other techniques to bypass these limitations.

6.2.9 The next hop of BGP announcements must correspond to the IP address assigned to the connection.

6.2.10 Participants undertake to:

6.2.10.1 announce prefixes in aggregated form,

6.2.10.2 minimize the announcement of specific prefixes.

6.2.11 Participants must keep the ROUTE and ROUTE6 objects updated in the Internet Routing Registries (IRR) and inform Namex of the IRRs used.

6.2.12 Participants are encouraged to implement and maintain valid RPKI ROA records for the announced prefixes.

6.2.13 Participants undertake to monitor the stability of the announcements (route flap) and to keep it within quality levels recognized by the Internet community.

6.2.14 Participants shall adopt all necessary measures to prevent their own traffic or that of their customers from compromising the stability and security of the platform.

6.2.15 Participants must disable on their devices, where not necessary:

6.2.15.1 Proxy ARP

6.2.15.2 ICMP Redirect

6.2.15.3 IP Directed Broadcast

6.2.15.4 Spanning Tree IEEE 802.1D

6.2.15.5 any protocol that generates uncontrolled broadcast or multicast traffic, with the exception of ARP and protocols strictly necessary for the proper functioning of the platform.

6.2.16 Participants must configure their devices to ensure the stability of the LAN, avoiding anomalous or excessive traffic, and collaborate with Namex in resolving any incidents.

6.2.17 Interfaces of routers connected to the peering LAN must be configured with an MTU of 1500 bytes. The Participant is required to ensure that this configuration is consistent across all devices involved in the connection to the platform, in order to guarantee the proper functioning of the service and the stability of the peering LAN.

6.2.18 Namex may apply control and protection mechanisms, such as rate-limiting broadcast, multicast, or unknown unicast traffic, in order to guarantee network stability.

6.3 Virtual-PNI (VPNI) and Closed User Group (CLUG) Services

6.3.1 Virtual-PNI (VPNI) and Closed User Group (CLUG) services are active private interconnection services that enable two or more Participants, following the setup of one or more connections to the active interconnection platform, to access a dedicated Layer 2 domain, separated from the public peering LAN, aimed at exchanging IP traffic in a private and segregated manner. These services may also be used for commercial purposes, such as providing IP transit, accessing dedicated services or applications, and establishing private interconnections between networks.

6.3.2 Participants may establish one or more connections to the active interconnection platform dedicated to VPNI and CLUG services, or use the same connection to access both the public peering service and private interconnection services, in compliance with the technical configurations defined by Namex.

6.3.3 The VPNI service involves the creation of an end-to-end VLAN between two Participants. For administrative and billing purposes, one of the two Participants is identified as the service initiator and is responsible for the financial aspects, while the other is identified as the user.

6.3.4 The CLUG service involves the creation of an extended VLAN among three or more Participants. For administrative and billing purposes, one of the Participants is identified as the service initiator and is responsible for the financial aspects, while the others are identified as users.

6.3.5 VPNI and CLUG services are identified, at the Participant's logical connection level, by specific VLAN tags assigned by Namex based on resource availability and its own management policies.

6.3.6 IP addressing used in VPNI and CLUG services is the sole responsibility of the participating Participants.

6.3.7 Participants are responsible for the configuration, security, and management of their own Layer 2 and Layer 3 domains, as well as for the traffic transported within the services.

6.3.8 Unless otherwise specified, Namex does not apply default limits to the number of MAC addresses visible behind a logical access connection to the service. However, Namex reserves the right to introduce limitations or protection measures if the network traffic or behavior compromises the stability or security of the platform.

6.4 Remote-IXP Service

6.4.1 The Remote-IXP service allows a Participant to access public peering services offered by other Internet Exchange Points by activating one or more virtual ports on remote platforms, using a connection to Namex's active interconnection platform.

6.4.2 The service includes the transport of traffic from the Namex node to the remote IXP's Point of Presence, via transport infrastructure and services provided by third parties or Namex. The list of available IXPs is provided in the Technical Appendices.

6.4.3 Participants must establish one or more connections to the active interconnection platform dedicated to accessing Remote-IXP services. These connections cannot be used to access other platform services, unless otherwise indicated by Namex.

6.4.4 Multiple remote interconnection services can be activated on the same connection. In this case, each service is identified by a VLAN tag assigned by the remote partner IXP or by Namex, depending on the technical methods adopted.

6.4.5 IP addressing associated with each remote interconnection service is assigned by the remote partner IXP. Generally, each service is required to be associated with a unique MAC address, consistent with the assigned IP addressing.

6.4.6 For each activated service, the Participant undertakes to comply with the technical, operational, and security policies defined by the remote IXP, including any requirements relating to device configuration, BGP security, and operational procedures.

6.4.7 Namex is not responsible for the quality, availability, or continuity of the services provided by the remote IXP or the involved transport providers, except as explicitly provided for in the applicable contractual agreements.

6.4.8 Any service disruptions, technical variations, or operational changes introduced by the remote IXP or transport providers may result in modifications to the service features. Namex will inform Participants using appropriate methods and timelines.

6.4.9 The Participant is responsible for the proper configuration of its equipment and the management of BGP sessions toward the remote IXP, as well as for compliance with applicable best practices and policies.

6.4.10 Namex reserves the right to suspend or limit the service in case of non-compliant use, risk to platform stability, or violation of applicable policies.

6.5 Remote Customer Aggregation Service

6.5.1 The Remote Customer Aggregation service, or reseller service, allows a Participant, acting as a reseller, to transport traffic from one or more remote customers from its own infrastructure to a Namex Point of Presence, in order to enable these customers to access some of the services offered by Namex.

6.5.2 The reseller must establish one or more connections to the remote aggregation platform, in accordance with the technical procedures defined by Namex.

6.5.3 For each connection, remote customers are identified by a unique VLAN tag, assigned by Namex based on resource availability and management policies.

6.5.4 The reseller is fully responsible to Namex for the traffic generated and the configurations of the transported remote customers, as well as for their compliance with these Technical Regulations.

6.5.5 The reseller must ensure that remote customers meet the technical, operational, and security requirements established by Namex for the services used.

6.5.6 The reseller must maintain an updated list of remote customers and provide it to Namex upon request, along with the technical information necessary for operational management and any troubleshooting or security activities.

6.5.7 Namex reserves the right to request the deactivation or restriction of the service for specific remote customers should they fail to comply with technical policies or compromise the stability, security, or integrity of the platform.

6.5.8 The reseller must ensure the adoption of adequate security measures, including BGP filtering policies, announcement control, and incident management.

6.5.9 The reseller is responsible for managing the IP addresses, routing resources, and BGP sessions of remote customers, as well as ensuring compliance with Internet community best practices.

6.5.10 Namex may request the implementation of specific technical or operational measures to ensure the security and stability of the service.

7 Violation of these regulations

7.1 Namex reserves the right to verify, at any time, compliance with the provisions of these Technical Regulations by Participants, including through requests for information, documentation, or technical evidence.

7.2 Participants are required to actively cooperate with Namex in verification, troubleshooting, and incident management activities, providing requested information in a timely manner.

7.3 The following constitute violations of these Regulations, including but not limited to:

7.3.1 behaviors that compromise the stability, security, or integrity of the interconnection platform,

7.3.2 incorrect configurations or those non-compliant with technical best practices,

7.3.3 unauthorized or invalid routing announcements, including route leaks and hijacking,

7.3.4 failure to comply with security, routing, or infrastructure usage policies,

7.3.5 improper or unauthorized use of Namex services,

7.3.6 failure to cooperate in managing technical or security incidents,

7.3.7 failure to communicate and/or update emergency contact details.

7.4 In the event of a violation of these Regulations, or behaviors that may compromise the stability, security, or integrity of the infrastructure or services, Namex shall adopt measures proportionate to the severity, urgency, and persistence of the situation, according to the following progression, except for the cases referred to in Article 7.5 below:

7.4.1 notice to the Participant's technical representative and operational contact, requesting analysis or the adoption of corrective measures within the specified timeframe,

7.4.2 application of temporary technical mitigation or containment measures, including selective traffic limitations, filtering, or other actions necessary to prevent impacts on the platform,

7.4.3 temporary limitation of specific services or connections affected by the violation,

7.4.4 temporary suspension of one or more of the Participant's connections or services,

7.4.5 Referral to the Technical Committee for further assessment and any consequent determinations, including any additional corrective or disciplinary actions.

7.5 In the event of serious or repeated violations, or where the situation poses an immediate risk to the security, stability, or integrity of the infrastructure or services, Namex may take action without prior notice by directly implementing the technical measures it deems necessary, including the immediate restriction or disconnection of the Participant or the services concerned, promptly notifying the contacts designated by the Participant.

7.6 Namex shall cooperate with the Participant to resolve the situation and restore normal operating conditions as soon as the circumstances that gave rise to the intervention have ceased.