IP PEERING POLICY

Bullroar Telecom, Ltd.

Autonomous System AS401673

Effective Date: 05/12/2026

---

1. COMPANY INFORMATION AND CONTACT DETAILS

Legal Entity: Bullroar Telecom, Ltd.

Autonomous System Number: AS401673

Business Address: PO Box 2226, Mandeville, LA 70470

Jurisdiction: Covington, Louisiana

Primary Peering Contact:

Aaron Wickware

Email: daw@bullroartel.com

Network Operations Center:

Phone: 504-962-3252

Email: noc@bullroartel.com

Peering Request Submissions:

Email: noc@bullroartel.com

---

2. PURPOSE AND SCOPE

2.1 Policy Objectives

This IP Peering Policy establishes the terms, conditions, and procedures under which Bullroar Telecom, Ltd. (“Company”) will enter into settlement-free peering arrangements with other autonomous systems. The primary purpose of this policy is to establish mutual traffic exchange relationships that improve network performance, reduce transit costs, and enhance the overall quality of internet connectivity for our customers and the broader internet community.

2.2 Regulatory Framework

This policy operates within the framework established by the Communications Act of 1934, as amended (47 U.S.C. § 151 et seq.), and federal interconnection requirements under 47 U.S.C. §§ 251-252. All peering arrangements shall comply with applicable federal telecommunications regulations and Louisiana state law governing commercial relationships.

2.3 Geographic Scope

Company seeks to establish peering relationships at major internet exchange points worldwide, with initial focus on our current points of presence at Dartpoints BTR2 and Hurricane Electric Fremont 2. Additional exchange points may be added at Company's discretion based on network expansion and strategic requirements.

---

3. PEERING REQUIREMENTS AND ELIGIBILITY

3.1 General Eligibility Criteria

To be eligible for peering with Company, potential peers must meet the following minimum requirements:

a) **Autonomous System Registration:** Possess a valid, registered Autonomous System Number (ASN) from an appropriate Regional Internet Registry (RIR)

b) **IP Address Resources:** Maintain legitimate IP address allocations or assignments from recognized internet registries

c) **BGP Capability:** Demonstrate technical capability to establish and maintain Border Gateway Protocol (BGP) sessions

d) **PeeringDB Registration:** Maintain an active, current, and accurate entry in PeeringDB.com with complete contact information, network details, and peering policies

e) **Legal Standing:** Operate as a legitimate telecommunications or internet service provider with proper business registration and licensing as required by applicable jurisdictions

3.2 Network Size and Traffic Requirements

Company evaluates potential peers based on mutual benefit regardless of network size. No specific minimum network size requirements are established. Evaluation criteria include:

a) **Traffic Patterns:** Complementary traffic patterns that provide mutual benefit to both networks

b) **Geographic Presence:** Network presence at common internet exchange points or potential for future co-location

c) **Technical Competence:** Demonstrated ability to maintain stable, secure network operations

d) **Business Relationship Potential:** Opportunity for long-term, mutually beneficial peering relationship

3.3 Settlement-Free Arrangement

All peering relationships established under this policy shall be settlement-free, meaning no monetary compensation shall be exchanged between parties for the mutual exchange of traffic. Each party bears its own costs for equipment, circuits, and operational expenses related to the peering arrangement. Third party costs, such as cross connects, will be negotiated an preferably split between the parties.

---

4. TECHNICAL REQUIREMENTS

4.1 Minimum Bandwidth Capacity

All peering connections must maintain a minimum bandwidth capacity of 10 Gigabits per second (10 Gbps). Higher capacity connections are encouraged and may be required based on traffic volumes and mutual agreement between parties.

4.2 Internet Exchange Point Requirements

Peering connections shall be established at mutually accessible internet exchange points. Company currently maintains presence at:

a) **Dartpoints BTR2**

b) **Hurricane Electric Fremont 2**

Additional exchange points may be considered based on mutual interest and technical feasibility. Each party is responsible for their own port costs, cross-connects, and equipment at exchange points.

4.3 BGP Configuration and Route Filtering

All peers must implement and maintain the following BGP requirements:

a) **Route Filtering:** Implement comprehensive route filtering to accept only legitimate routes and prevent route leaks. Peers must filter routes based on:

- Registered route objects in Internet Routing Registries (IRR)
- Resource Public Key Infrastructure (RPKI) validation
- Prefix length limitations (typically /24 maximum for IPv4, /48 maximum for IPv6)
- AS-path filtering to prevent transit traffic

b) **RPKI Validation:** Mandatory implementation of Resource Public Key Infrastructure (RPKI) validation for all route announcements. Peers must:

- Maintain valid Route Origin Authorizations (ROAs) for all announced prefixes
- Implement RPKI validation in their BGP decision process
- Reject invalid routes based on RPKI validation results

c) **BGP Security Measures:** Implement industry-standard BGP security practices including:

- MD5 authentication for BGP sessions where supported
- Prefix filtering based on documented network policies
- AS-path filtering to prevent unauthorized transit
- Regular monitoring of route announcements and withdrawals

4.4 IP Address Announcements

Company will announce the following IP address ranges to peering partners: [To be completed based on current allocations and routing policy]. Peers must provide complete documentation of their intended route announcements prior to establishing peering sessions.

4.5 IPv6 Support

While not mandatory, IPv6 peering is strongly encouraged. Peers implementing IPv6 must follow the same security and filtering requirements as specified for IPv4, with appropriate modifications for IPv6 address space and routing practices.

---

5. TRAFFIC EXCHANGE TERMS

5.1 Traffic Ratio Policy

Company maintains a flexible approach to traffic ratios between peering partners. While no strict ratio requirements are enforced, Company reserves the right to:

a) **Periodic Review:** Conduct periodic reviews of traffic patterns and ratios with peering partners

b) **Discussion and Adjustment:** Engage in good faith discussions regarding significant traffic imbalances that may affect network performance or economics

c) **Mutual Benefit Assessment:** Evaluate whether traffic exchange continues to provide mutual benefit to both parties

d) **Modification Rights:** Request modifications to peering arrangements if traffic patterns significantly deviate from expected norms or create operational challenges

5.2 Traffic Types and Restrictions

Peering arrangements cover the exchange of internet traffic between the respective customer bases of each network. The following restrictions apply:

a) **Customer Traffic Only:** Peering is limited to traffic destined for or originating from each party's direct customers

b) **No Transit Traffic:** Neither party shall send transit traffic (traffic from third-party networks) across the peering connection

c) **Prohibited Content:** Peers must implement reasonable measures to prevent the transmission of illegal content, spam, or malicious traffic

d) **Quality of Service:** While no specific Quality of Service (QoS) guarantees are provided, both parties agree to maintain reasonable network performance standards

5.3 Capacity Management

Both parties agree to:

a) **Monitor Utilization:** Regularly monitor peering link utilization and performance metrics

b) **Capacity Upgrades:** Engage in discussions regarding capacity upgrades when sustained utilization exceeds 80% of available bandwidth

c) **Proactive Planning:** Provide reasonable advance notice of anticipated traffic growth that may require capacity adjustments

---

6. OPERATIONAL SUPPORT REQUIREMENTS

6.1 Support Hours and Availability

Company provides operational support during standard business hours (Monday through Friday, 8:00 AM to 5:00 PM Central Time, excluding federal holidays). Peers are expected to maintain similar support availability for routine operational matters.

6.2 Emergency Contact Procedures

For critical issues affecting network connectivity or security, Company maintains emergency contact procedures:

a) **Emergency Contacts:** Each peer must provide 24/7 emergency contact information for critical network issues

b) **Escalation Procedures:** Clear escalation procedures must be established for issues requiring immediate attention

c) **Response Time Expectations:** Emergency contacts should respond to critical issues within two (2) hours of notification

d) **Communication Methods:** Multiple communication methods (phone, email, SMS) should be available for emergency situations

6.3 Planned Maintenance Coordination

Both parties agree to:

a) **Advance Notice:** Provide minimum 72-hour advance notice for planned maintenance affecting peering connections

b) **Maintenance Windows:** Schedule maintenance during mutually agreed upon low-traffic periods when possible

c) **Emergency Maintenance:** For emergency maintenance, provide notice as soon as reasonably possible

d) **Documentation:** Maintain records of maintenance activities and their impact on peering relationships

6.4 Network Operations Center Requirements

Each peer must maintain or have access to qualified network operations personnel capable of:

a) **BGP Troubleshooting:** Diagnosing and resolving BGP session issues

b) **Route Analysis:** Analyzing routing tables and identifying routing problems

c) **Security Response:** Responding to security incidents and implementing protective measures

d) **Performance Monitoring:** Monitoring network performance and identifying capacity issues

---

7. SECURITY AND ABUSE PREVENTION

7.1 Security Incident Response

All peering partners must cooperate in security incident response activities according to the following requirements:

a) **Incident Notification:** Promptly notify Company of any security incidents that may affect peering connections or traffic exchange

b) **Cooperative Investigation:** Participate in good faith investigations of security incidents, including providing relevant log data and technical information as legally permissible

c) **Remediation Efforts:** Take prompt action to remediate security vulnerabilities or abuse issues identified through the peering relationship

d) **Information Sharing:** Share relevant threat intelligence and security information that may benefit both networks, subject to confidentiality requirements

7.2 Escalation Procedures

Security incident escalation follows these defined procedures:

a) **Initial Contact:** Security incidents should be reported to noc@bullroartel.com with "SECURITY INCIDENT" in the subject line

b) **Severity Classification:** Incidents will be classified as Critical, High, Medium, or Low based on potential impact to network operations

c) **Response Timeline:**

- Critical incidents: Response within 1 hour
- High severity: Response within 4 hours
- Medium severity: Response within 24 hours
- Low severity: Response within 72 hours

d) **Escalation Path:** Unresolved incidents will be escalated to senior technical staff and management as appropriate

7.3 Abuse Prevention and Response

Both parties agree to implement reasonable measures to prevent and respond to network abuse:

a) **Abuse Contacts:** Maintain current abuse contact information in relevant databases (WHOIS, PeeringDB)

b) **Abuse Response:** Respond to legitimate abuse complaints within 24 hours of receipt

c) **Preventive Measures:** Implement appropriate technical and procedural measures to prevent abuse originating from their networks

d) **Cooperation:** Cooperate with law enforcement and other authorities in investigating abuse and illegal activities as required by law

7.4 Immediate Suspension Authority

Company reserves the right to immediately suspend peering connections in the following circumstances:

a) **Security Threats:** Active security threats emanating from the peer's network

b) **Abuse Activities:** Ongoing abuse activities that are not promptly addressed

c) **Route Hijacking:** Unauthorized announcement of Company's IP address space

d) **BGP Attacks:** Malicious BGP activities including route leaks or path manipulation

e) **Legal Requirements:** When required by court order, law enforcement directive, or regulatory mandate

---

8. MODIFICATION AND TERMINATION PROCEDURES

8.1 Non-Emergency Modifications and Termination

For non-emergency modifications or termination of peering relationships, the following procedures apply:

a) **Advance Notice Requirement:** Either party may modify or terminate the peering relationship by providing thirty (30) days written notice to the other party

b) **Notice Format:** Written notice must be provided via email to the designated peering contact and confirmed by telephone or alternative communication method

c) **Reason Documentation:** Notice should include the reason for modification or termination and any proposed alternative arrangements

d) **Transition Period:** During the notice period, both parties agree to maintain existing service levels and cooperate in orderly transition planning

e) **Final Disconnection:** Physical disconnection of peering circuits shall occur no earlier than the expiration of the notice period unless mutually agreed otherwise

8.2 Emergency Suspension Procedures

In accordance with 47 C.F.R. Part 51 and applicable federal telecommunications regulations, Company may immediately suspend peering connections for:

a) **Immediate Security Threats:** Active attacks, malware distribution, or other security threats requiring immediate response

b) **Network Stability Issues:** Technical problems that threaten the stability or performance of Company's network

c) **Legal Compliance:** Requirements to comply with court orders, law enforcement directives, or regulatory mandates

d) **Breach of Policy:** Material violations of this peering policy that pose immediate risk to network operations

8.3 Reinstatement Procedures

Following emergency suspension, peering connections may be reinstated when:

a) **Issue Resolution:** The underlying cause of suspension has been identified and resolved

b) **Verification:** Company has verified that appropriate corrective measures have been implemented

c) **Compliance Confirmation:** The peer has confirmed compliance with all applicable policy requirements

d) **Technical Testing:** Successful completion of technical testing to ensure proper operation

8.4 Post-Termination Obligations

Following termination of peering relationships:

a) **Route Withdrawal:** Both parties must promptly withdraw all routes learned through the terminated peering session

b) **Equipment Removal:** Each party is responsible for removing their equipment from shared facilities within thirty (30) days

c) **Data Retention:** Traffic and routing data may be retained for legitimate business purposes in accordance with applicable data retention policies

d) **Confidentiality:** Ongoing obligations regarding confidential information shall survive termination

---

9. DISPUTE RESOLUTION

9.1 Good Faith Negotiation Requirement

In accordance with Louisiana Civil Code Article 1906 and general contract principles, all disputes arising from or relating to peering relationships must first be addressed through good faith negotiation between the parties:

a) **Direct Communication:** Disputes should initially be addressed through direct communication between designated technical contacts

b) **Management Escalation:** If technical contacts cannot resolve the dispute within five (5) business days, the matter shall be escalated to management representatives

c) **Documentation:** All dispute resolution efforts must be documented in writing, including proposed solutions and reasons for rejection

d) **Timeline:** Good faith negotiation efforts should continue for a minimum of fifteen (15) business days before proceeding to formal dispute resolution

9.2 Mediation Procedures

If good faith negotiation fails to resolve disputes, the parties agree to participate in mediation:

a) **Mediator Selection:** The parties shall mutually select a qualified mediator with experience in telecommunications or internet infrastructure disputes

b) **Mediation Location:** Mediation shall be conducted in Covington, Louisiana, or via electronic means if mutually agreed

c) **Cost Sharing:** The costs of mediation shall be shared equally between the parties

d) **Confidentiality:** All mediation proceedings shall be confidential and inadmissible in any subsequent legal proceedings

e) **Timeline:** Mediation should be completed within thirty (30) days of the mediator's appointment

9.3 Interim Measures

During dispute resolution proceedings:

a) **Service Continuity:** Both parties agree to maintain existing service levels unless safety or security concerns require immediate action

b) **No Retaliation:** Neither party shall take retaliatory actions that could harm the other party's network operations

c) **Information Preservation:** Both parties shall preserve relevant documentation and technical data related to the dispute

d) **Communication Protocol:** All dispute-related communications shall be conducted through designated representatives

9.4 Resolution Implementation

Upon successful dispute resolution:

a) **Written Agreement:** All resolutions must be documented in a written agreement signed by authorized representatives

b) **Implementation Timeline:** Specific timelines for implementing agreed-upon solutions must be established

c) **Monitoring:** Both parties agree to monitor compliance with dispute resolution agreements

d) **Future Prevention:** Parties should identify and implement measures to prevent similar disputes in the future

---

10. COMPLIANCE AND REPORTING REQUIREMENTS

10.1 PeeringDB Registration Requirements

All peering partners must maintain compliance with the following PeeringDB requirements:

a) **Active Registration:** Maintain an active, current, and accurate entry in PeeringDB.com at all times during the peering relationship

b) **Information Accuracy:** Ensure all contact information, network details, peering policies, and technical specifications are current and accurate

c) **Regular Updates:** Update PeeringDB information within ten (10) business days of any material changes to network configuration, contact information, or peering policies

d) **Verification:** Provide PeeringDB registration details to Company upon request for verification purposes

e) **Public Information:** Maintain appropriate public visibility of peering information to facilitate industry coordination

10.2 Contact Information Maintenance

Peering partners must maintain current contact information according to these requirements:

a) **Primary Contacts:** Provide and maintain current information for primary peering contacts, including name, title, email address, and telephone number

b) **Technical Contacts:** Maintain 24/7 technical contact information for network operations and emergency response

c) **Administrative Contacts:** Provide administrative contact information for business and legal matters

d) **Update Notifications:** Notify Company within five (5) business days of any changes to contact information

e) **Annual Verification:** Confirm accuracy of all contact information on an annual basis

10.3 Annual Compliance Confirmation

Each peering partner must provide annual confirmation of continued compliance with this policy:

a) **Annual Review:** Conduct annual review of compliance with all policy requirements

b) **Certification:** Provide written certification of continued compliance signed by an authorized representative

c) **Documentation Updates:** Submit any necessary updates to technical specifications, network configurations, or operational procedures

d) **Policy Acknowledgment:** Acknowledge receipt and understanding of any policy updates or modifications

e) **Due Date:** Annual compliance confirmation is due within thirty (30) days of the anniversary of the peering relationship establishment

10.4 Audit and Verification Rights

Company reserves the right to conduct reasonable audits and verification activities:

a) **Technical Audits:** Verify compliance with technical requirements including BGP configuration, route filtering, and security measures

b) **Documentation Review:** Review relevant documentation to confirm compliance with operational and administrative requirements

c) **Performance Monitoring:** Monitor peering connection performance and traffic patterns to ensure compliance with policy terms

d) **Notice Requirements:** Provide reasonable advance notice of audit activities except in emergency situations

e) **Cooperation:** Peering partners agree to cooperate with reasonable audit and verification requests

10.5 Non-Compliance Remediation

In cases of non-compliance with policy requirements:

a) **Notice of Non-Compliance:** Company will provide written notice of identified non-compliance issues

b) **Cure Period:** Peering partners have fifteen (15) business days to cure non-compliance issues unless immediate action is required for security reasons

c) **Remediation Plan:** For complex issues, partners may submit a remediation plan with specific timelines for achieving compliance

d) **Monitoring:** Company will monitor remediation efforts and provide reasonable assistance when appropriate

e) **Escalation:** Persistent non-compliance may result in modification or termination of the peering relationship

---

11. GENERAL PROVISIONS

11.1 Governing Law and Jurisdiction

This IP Peering Policy and all peering relationships established hereunder shall be governed by and construed in accordance with the laws of the State of Louisiana, without regard to conflict of law principles. In accordance with Louisiana Civil Code Articles 1756-2057, all contractual relationships arising from this policy shall be subject to Louisiana contract law principles. Any legal proceedings arising from or relating to this policy or peering relationships shall be subject to the jurisdiction of the courts of Covington, Louisiana.

11.2 Entire Agreement and Modifications

This IP Peering Policy, together with any specific peering agreements executed between the parties, constitutes the entire agreement between Company and each peering partner regarding the subject matter hereof. This policy supersedes all prior negotiations, representations, or agreements relating to peering arrangements. Modifications to this policy must be made in

writing and signed by authorized representatives of Company. Company reserves the right to modify this policy with thirty (30) days advance notice to existing peering partners.

11.3 Severability and Enforceability

If any provision of this policy, or any portion thereof, is held to be invalid, illegal, void, or unenforceable by any court or tribunal of competent jurisdiction, the remainder of this policy shall remain in full force and effect to the maximum extent permitted by law. The parties agree that any such invalid, illegal, void, or unenforceable provision shall be modified and limited in its effect to the extent necessary to cause it to be enforceable, or if such modification is not possible, shall be deemed severed from this policy. In such event, Company shall have the right to modify the policy to replace any invalid, illegal, void, or unenforceable provision with a valid, legal, and enforceable provision that corresponds as closely as possible to the original intent and economic expectations. The invalidity or unenforceability of any provision in one jurisdiction shall not affect the validity or enforceability of such provision in any other jurisdiction.

11.4 Force Majeure

Neither party shall be liable for any failure or delay in performance under this policy that is due to fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism, or any other cause beyond the reasonable control of such party, provided that such party uses reasonable efforts to notify the other party of such force majeure event and to cure the effects thereof as soon as reasonably practicable.

11.5 Independent Contractor Relationship

The relationship between Company and each peering partner is that of independent contractors. Nothing in this policy shall be construed to create a partnership, joint venture, agency relationship, or employment relationship between the parties. Neither party has the authority to bind the other party or to incur obligations on behalf of the other party without express written consent.

11.6 Confidentiality

Each party acknowledges that it may have access to certain confidential information of the other party in connection with the peering relationship. Each party agrees to maintain the confidentiality of such information and to use it solely for the purposes of the peering relationship. This obligation shall survive termination of the peering relationship for a period of three (3) years.

11.7 Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, LOSS OF DATA, OR BUSINESS INTERRUPTION, ARISING FROM OR RELATING TO THIS POLICY OR ANY PEERING RELATIONSHIP, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.8 Notices

All notices required or permitted under this policy must be in writing and shall be deemed given when: (a) delivered personally; (b) sent by confirmed facsimile transmission; (c) sent by confirmed electronic mail to the designated email addresses; or (d) sent by certified or registered mail, return receipt requested, postage prepaid, to the addresses specified in this policy or as subsequently updated by written notice.

11.9 Waiver

No waiver of any provision of this policy shall be deemed or shall constitute a waiver of any other provision. No waiver shall be effective unless it is in writing and signed by the party making the waiver. No failure or delay by either party in exercising any right, power, or privilege under this policy shall operate as a waiver thereof.

11.10 Assignment

Neither party may assign its rights or obligations under this policy without the prior written consent of the other party, except that either party may assign this policy to an affiliate or in connection with a merger, acquisition, or sale of all or substantially all of its assets related to the network operations covered by this policy.

11.11 Survival

The provisions of this policy relating to confidentiality, limitation of liability, governing law, dispute resolution, and any other provisions that by their nature should survive termination shall survive any termination or expiration of peering relationships established under this policy.

Document Version: 1.0

Last Updated: 05/12/2026

Next Review Date: 05/12/2027

Authorized Representative:

Bullroar Telecom, Ltd.

By: 

Name: Aaron Wickware

Title: President

Date: 05/12/2026