



## LVT Corp dba Lynxx Networks - Network Transparency Statement

LVT Corp dba Lynxx Networks (also referred to in this document as “Lynxx Networks” or “Company”) provides this Network Transparency Statement in accordance with the FCC’s Restore Internet Freedom Rules to ensure that customers have sufficient information to make informed choices about the purchase of broadband services. Information about Lynxx Networks’ other policies and practices concerning broadband are available at [www.getlynxx.com](http://www.getlynxx.com) (the Lynxx Networks website).

Lynxx Networks engages in network management practices that are tailored to and appropriate for achieving optimization of the network. Lynxx Networks’ goal is to ensure that all customers experience a safe and secure broadband Internet environment that is fast, reliable, and affordable.

Lynxx Networks’ network management practices include congestion- and security-protocol-management. Customers will generally not be impacted by the practices and protocols that Lynxx Networks uses to manage its network.

### **A) Lynxx Networks’ Network Transparency Disclosures**

Lynxx Networks uses various tools and industry standard techniques to manage its network and deliver fast, secure, and reliable Internet service. Lynxx Networks believes in full transparency and provides the following disclosures about its network management practices:

**Blocking:** Lynxx Networks does not block or discriminate against lawful content.

**Throttling:** Lynxx Networks does not throttle, impair or degrade lawful Internet traffic.

**Affiliated Prioritization:** Lynxx Networks does not prioritize Internet traffic and has no plans to do so.

**Paid Prioritization:** Lynxx Networks has never engaged in paid prioritization. Lynxx Networks does not prioritize Internet to benefit particular content, applications, services, or devices. Lynxx Networks does not have plans to enter into paid prioritization deals to create fast lanes.

**Congestion Management:** Lynxx Networks monitors the connections on its network in the aggregate on a continuous basis to determine the rate of utilization. If congestion emerges on the network, Lynxx Networks will take the appropriate measures to relieve congestion.

Customers have access to all legal services, applications, and online content and, in the event of

congestion, most Internet activities will be unaffected. However, some customers may experience longer download or upload times, or slower surf speeds on the web if instances of congestion do occur. Lynxx Networks' congestion management practices are 'application-agnostic' and based on real-time network conditions. Congestion management practices are not implemented based on customers' online activities, protocols, or applications and do not relate to any customer's aggregate monthly data usage.

**Application-Specific Behavior:** Except as may be provided elsewhere herein, Lynxx Networks does not currently engage in any application-specific behaviors on its network. Customers may use any lawful applications on the network.

**Device Attachment Rules:** For best results, wireless routers or other proprietary network gateways used on Lynxx Networks' broadband network should be provided by Lynxx Networks. Customers may attach their own devices, including wired or wireless routers, laptops, desktop computers, video game systems, televisions, or other network-enabled electronics equipment. However, customers are responsible for ensuring that their equipment does not harm Lynxx Networks' network or impair the service of other customers. Lynxx Networks is not responsible for the functionality or compatibility of any equipment provided by its customers. Customers are responsible for securing their own equipment to prevent unauthorized access to Lynxx Networks' broadband by third parties and will be held responsible for the actions of such third parties who gain unauthorized access through unsecured customer equipment.

**Network Security:** Lynxx Networks is committed to securing its network and customers from online threats and annoyances. The company employs several security practices to help guard against threats and protect the integrity and availability of its network. Lynxx Networks deploys email spam filters to automatically quarantine inbound messages flagged as spam. Quarantined messages are automatically deleted if not accessed within 30 days. Customers have the ability to whitelist messages that may be incorrectly flagged. Lynxx Networks requires encrypted and authenticated ports to send email and implements outbound email policies to prevent the origination and propagation of spam. When a customer's outbound email traffic exceeds thresholds for the following metrics, the associated account will be added to a temporary email blacklist until the traffic returns to normal levels:

- Recipients per message
- Recipients per hour
- Recipients per connection
- Simultaneous or concurrent connections

As its normal practice, Lynxx Networks does not block any protocols, content, or traffic for purposes of network management. Lynxx Networks may block or limit traffic that is deemed to be associated with spam, virus propagation, malware propagation, or denial of service attacks to protect network integrity and the security of its customers. Lynxx Networks monitors for abnormal traffic flows that may indicate potential network security breaches, malware propagation, and loss or damage to the network. If a breach is detected, Lynxx Networks provides notification to the impacted customer(s) via e-mail or phone. If a violation of Lynxx

Networks' policies has occurred and such violation is not remedied, Lynxx Networks will seek to suspend or terminate the offending customer's service.

Customers engaging in conduct that abuses or threatens Lynxx Networks' network or that violates the company's Acceptable Use Policy, Internet Service Terms and Conditions, or the Internet Service Agreement will be asked to stop any such activity immediately. A failure to respond or to cease any such conduct could result in service suspension or termination.

## **B) Network Performance**

**Service Descriptions:** Lynxx Networks deploys Internet access to its subscribers through a fixed wired broadband network (Fiber Optic Network/Fiber to the Premise).

**Network Performance:** Lynxx Networks makes every effort to support advertised broadband speeds and will dispatch repair technicians to customer sites to perform speed tests as needed to troubleshoot and resolve speed and performance issues caused by Lynxx Networks' network. Lynxx Networks measures availability, latency, and aggregate utilization on the network to ensure reliability. However, the speed at which distant websites or other Internet resources may be downloaded, or the speed at which customer information may be uploaded to distant websites or Internet locations is affected by factors beyond Lynxx Networks' control. This includes the speed of the connection from distant web servers to the Internet, congestion on intermediate networks, and/or limitations on customer owned equipment, including wireless routers, PCs, and other devices. In addition, service performance may be affected by the inside wiring and/or the quality of the wireless network at a customer premise. Customers must consider the capabilities of their equipment when choosing a Lynxx Networks broadband service. Customer-owned devices and wireless or wired networks may need to be upgraded to take full advantage of the chosen Lynxx Networks broadband plan. Lynxx Networks tests each service for actual and expected access speeds at the time of network installation to demonstrate that the service can support the advertised speed. Customers may test broadband speeds by using the Bandwidth Test option in the Lynxx Command IQ application or by using web-based speed tests such as the one found Lynxx Networks website: <https://speedtest.airstreamcomm.net>. Customers may request assistance by calling the business office at 608.427.6515 or by emailing [info@getlynxx.com](mailto:info@getlynxx.com).

**Impact of Non-BIAS Data Services:** The FCC has defined Non-Broadband Internet Access Services (Non-BIAS) to include services offered by broadband providers that share capacity with Broadband Internet Access Services (BIAS) (previously known as "Specialized Services") also offered by the provider over last-mile facilities. Non-BIAS services, which include real-time services such as Voice over Internet Protocol (VoIP) and Internet Protocol (IP) video services, command optimal bandwidth. Lynxx Networks offers both VoIP and IP video services to customers. Priority is given to these Non-BIAS services over best-effort BIAS services where allowable. Customers should note that significantly heavier use of Non-BIAS services (particularly IP video services) may impact the available capacity for and/or the performance of BIAS services.

## **C) Terms**

Pricing and additional service information may be found at Lynxx Networks' website – [www.getlynxx.com](http://www.getlynxx.com).