CNSNEXT Open Internet Disclosure Statement

CNSNext, provides the following disclosure regarding our network management practices, as well as the performance and commercial terms of our broadband Internet access service. This disclosure is provided 1) to all customers to make informed choices regarding their use of our services and 2) to all content, application, service providers to develop, market and maintain Internet offerings. Unless otherwise specified, for purposes of this statement, "we" and "our" shall mean the CNSNext, and "You" shall apply to customers and end users.

Our Service and Performance

We use a variety of technologies to deliver broadband Internet access service to government, residential and business customers in our service areas. Our networks are fiber based, and we provide up to 10 Gig Ethernet and/or DOCSIS 3.1 cable service to customers in and around Cairo, Camilla, Moultrie and Thomasville, Georgia.

Based on internal testing or consumer speed data, a user's expected and actual access speed and latency will vary based on network conditions, congestion, other users on the network, the number of devices attached to an access point and other factors. Maximum speeds will be limited by these factors and in accordance with our congestion management practices as described below. We publish a link to a bandwidth test system, https://cns.speedtestcustom.com which provides not only speed but information about latency and jitter. We monitor and log all cable modem and Metro Ethernet traffic metrics. This is only the packet header and service flow information not the content. We log this information for future buildout projection analysis to eliminate bottlenecks.

For our cable networks, local congestion can affect the end user's experience due to the shared portions of the network. Under normal operations, average latency is 15 milliseconds, and if our monitor determines latency in excess of 30 milliseconds, we examine the connection to determine if there are problems. Under normal circumstances, our service is suitable for all real-time applications.

We offer end users facilities-based VoIP as a specialized service, and we add quality of service protections. While such services may affect the amount of last-mile capacity available for and the performance of broadband Internet access service, in practice this impact is very limited because of the high capacity available on our networks.

Congestion Management Practices

Providing quality broadband service requires that we take steps to provide reasonable management of our networks. Subject to reasonable network management, we do not degrade, impair access to, block or otherwise prevent end user access to lawful content, applications, services or non-harmful devices. We also have no practices that directly or indirectly favor some traffic over other traffic, whether to benefit an affiliate or in exchange for monetary or nonmonetary consideration.

Reasonable network management requires us to monitor and prevent malicious content, spam, viruses, and botnets as well as to handle congestion on our networks, as described below.

Multiple users share upstream and downstream bandwidth on our networks. We regularly monitor our networks for bandwidth usage. We frequently and automatically reconfigure and upgrade equipment to mitigate any bottlenecks. Any anomalies are reported to our Network Operations Center ("NOC") by monitoring servers which constantly monitor the network. As needed, we create filters, traps or other means to prevent virus and malware propagation.

In the ordinary course, a customer should experience congestion only when there's a problem with the network, not through normal usage. Accordingly, our customers are not usage-limited at this time. We do not implement monthly bandwidth usage caps like most other providers. Our congestion management techniques are triggered on a portion of our networks when we monitor our users' aggregate bandwidth usage and we identify those users who are in the top 2 percent based on our usage statistics. By using various network monitor facilities, we inspect this traffic to help determine if the user's connection is compromised by botnets, malware, or other malicious means. We will contact users as a courtesy if they fall into this high-usage category and we see a high level of peer-to-peer usage. We make these calls to customers 1) to confirm that the user is aware of the activity, and 2) to notify them of the effect this has on their internet experience with respect to botnet or potentially malicious data. In some instances, customers may experience degraded internet access, uploads, downloads, or slower response in real-time applications. In general, a customer should only experience congestion infrequently (i.e., when there's a problem with the network), not in the ordinary course.

We address application-specific behavior in our network practices. We block SMTP port 25 outbound unless a customer provides us with valid reasons for access to this port and completes an application form. Consistent with industry standards, this practice is in place to address concerns about use of this port to send high volumes of unsolicited email. In all other respects related to application-specific behavior, we do not modify protocol fields in ways not prescribed by the protocol standard, and we do not otherwise inhibit or favor certain applications or classes of applications.

We take seriously our commitment to the security of our network and of service to end users. To advance this goal, we engage in practices used to facilitate such security. For example, we assign dynamic IP addresses to all of our cable modem customers.

We also use monitoring to gather network statistics to aggregate and identify outlier parameters that may suggest content that is malicious or may cause unacceptable congestion in our networks. As needed, we create filters, traps or other means to prevent virus and malware propagation. All of our servers are behind firewalls, and we follow industry best practices to minimize applications that are running, ports open and types of traffic allowed. We use two-factor authentications for access, and all server logs are gathered, housed offsite and regularly monitored. In addition, we reserve the right to suspend or terminate a customer's access to our service for violations of our Internet Service Agreement or our Acceptable Use Policy.

Our service involves the inspection of network traffic to a limited extent. While we don't examine the content of user's traffic (e.g., the content of emails or of websites visited), we review aggregated traffic data to help us manage the network and to identify trouble issues. We store data related to IP addresses for one year, and any traffic information used for network management is provided to third parties only as required by law. Requests for such information must be accompanied by a signed and properly executed subpoena or other valid legal process. Information regarding customer privacy, including the protection of customer proprietary information is addressed in our privacy policy.

Commercial Terms

Information about our pricing terms is available here.

We have no usage-based fees, and we charge no fees for early termination because our service is provided on a month-to-month basis. We charge the following fees for additional network services:

Commercial Internet services have priority data on the network when network congestion is detected.

Commercial customers receive up to 1 Static IP free, based on the tier of service.

Additional Static IP addresses - $5.00 each per month (Limit of 4 IPs per account)

NextConnect Wi-Fi Service - $6.99 each month

If you have questions or complaints about our service, you can contact our Helpdesk. Our help desk number is 1-844-721-8029 or email support@cnsnext.com. Help requests for residential and small business customers get Level 1 helpdesk service. These technicians also have access to Level 2 Network Operations Engineers. Customers with Ethernet connections receive a Level 2 direct telephone number as part of their service package. Third parties can contact us through either means. Our goal is to resolve complaints effectively and expeditiously.

We reserve the right to make changes to our Open Internet policies. These changes will take effect when posted on our website.

Last modified: December 1st, 2023