Open Internet Disclosure Statement

The City of Cairo, Georgia, 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 City of Cairo, Georgia, 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 3.0 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 two different bandwidth test systems www.cns-internet.com/speedtest/, http://www.cns-internet.com:8000/speedtest, which provide not only speeds but information about latency and jitter. We monitor and log all cable modem and Metro Ethernet traffic. We log this information for future buildout to ensure no 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 network(s). Subject to reasonable network management, we do not block lawful content, applications, services or non-harmful devices, nor do we unreasonably discriminate in transmitting lawful network traffic over a consumer's broadband Internet access, again subject to our reasonable network management.

The purposes for our network management techniques are to monitor and prevent malicious content, spam and viruses, as well as to handle congestion on our networks, as described below.

At present, we do not have in place practices designed to reduce or eliminate congestion on our networks by artificially or automatically limiting our users' bandwidth consumption. 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. 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 when there's a problem with the network, not in the ordinary course.

We address application-specific behavior in our network practices. For example, 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.

We have limited restrictions on the types of devices that may access our networks and limited approval procedures for such devices. We have to approve a customer's cable modem if they want to purchase their own. The reason is that our network is optimized to take advantage of Turbo Boost features in Arris cable modems, and this feature is not available in all off-the-shelf modems.

We take seriously our commitment to 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, and these IP addresses are behind a carrier-class firewall. We do this to help prevent DDOS and other malicious attacks and to limit the spread of malware. Customers who prefer static IP addresses must provide us with a signed letter indicating that they understand that they

need to purchase their own firewall. Residential customers must pay a fee for this service; commercial customers are entitled to one free IP address that is not behind our firewall. We also use monitoring to gather network statistics to aggregate and identify outlier parameters that may suggest content that is malicious or may cause congestion in our networks. As needed, we create filters, traps or other means to prevent virus and malware propagation. All 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 authentication 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.

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:

Additional Emails	$2.50 per month, 5 emails free w/ account
Antivirus	$ .99 per month F-Secure
Internet Filtering	$2.99 per month
Residential Static IP	$2.50 per month
Networking 2 PC's	$99.95 (a 3rd PC will be an additional $69.95)
Wireless Installation	$149.95
Yellow Page Ad	$2.50/month

Domain Hosting
$25.00 (one time) Domain set up Fee if Domain is already reserved
$50.00 (one time) Domain set up Fee if Domain is NOT already reserved
$12.99 per month hosting 3.72GB storage
$16.99 per month hosting 3.72GB storage, SSL
$19.99 per month hosting 4GB storage, SSL
$26.99 per month hosting 6GB storage, SSL

Residential customers may opt out of dynamic address assignment and firewalls, and thus obtain an Internet routable address, for a fee of $2.50 per month. Commercial customers are entitled to one free IP address that is not behind our firewall and must pay a fee for additional IP addresses.

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., emails or 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.

If you have questions or complaints about our service, you can contact our help desk. Our help desk number is given to users, as well as published in the phone book and in marketing materials. 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 T-1 or 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: November 20, 2011