

## Network Management Policy

Crosslake Communications (the Company) invests significant resources to bring internet access to our customers and strives to provide customers an optimum online experience that enables them to access all available content, including: up-to-date news and information, online shopping, communications tools, movies, video, music, gaming and an array of other online services, all within the realm of the Open Internet principle. Generally, the Company utilizes a best-efforts approach to deliver Broadband Internet Access Service so that customers experience speeds at or near the advertised levels.

Key attribute of the Company's network management are:

- It does not block, throttle, or inhibit any specific applications or classes of applications.
- It does not directly or indirectly favor some traffic over other traffic for the benefit of an affiliate.
- It does not engage in paid prioritization.
- It does not restrict the types of devices that can be connected to its network.

Accordingly, this means that except as described in the Specialized Services section below, the Company does not prioritize one type of traffic or application over the other types, however, the continuing explosive growth in internet consumption may cause periodic congestion in the network that the Company must address. The Company uses network management tools to optimize quality of service to customers for applications that are sensitive to packet loss, delay or jitter like VoIP, time sensitive data, and video traffic.

Like other internet service providers, the Company manages its network to provide customers a secure and optimal internet experience. Generally, the Company monitors the flow of traffic on its network, including the amount of data sent to and from customer connections, the source and destination of data, and the type – but not the contents – of information sent and received. In limited circumstances, however, the Company may also review the contents of the information to determine whether it is malicious (such as spam or a virus) or when required by law. The Company continually upgrades its security and network management tools based on technology advances and network needs.

The Company generally allows customers to attach any lawful device to its network so long as it does not impede the provision of internet access service, harm the network, enable theft of the service or a violation of the Company's Acceptable use Policy or any terms of service, or harm other users of the service.

**Customer Privacy and Rights** Customers can consult the Company's general Customer Privacy and Rights of service as well as internet pricing plans for more information about their internet service.

### Service Performance

All company broadband internet access services are provided either by fiber, DSL, VDSL, DOCSIS or wireless technology. The technology for your service will be based upon what is available in your geographic area. Where DSL, VDSL or DOCSIS is used, speeds available may be dependent on your location. Service may not be available to all locations.

The service speeds identified in the Company's marketing materials and other communications reflect maximum advertised speed and services provided will be "up to" those advertised. Actual

speed experienced by a customer will vary based on multiple factors including inside wiring and customer equipment configuration, interference on the customer's line, website(s) accessed, and internet congestion.

#### Speed Test Link

Customers can determine the speed of their broadband internet access service connection at this link: <http://www.emily.net/st>.

Latency is highly variable depending on the network path, other providers in the path, the distance to the destination, and performance of end destination servers. Customers should expect roundtrip latency to most general internet sites be less than 100ms.

#### Specialized Services IP Video and VoIP

For certain customers, the Company offers specialized services, such as IP Video or Voice over IP ("VoIP"), over the same customer facilities as broadband internet access services. When the customer uses these specialized services, less bandwidth will be available for broadband internet access service than when they are not using the specialized service. When the specialized service is not in use, customers can, in most cases, use the full facility capacity for broadband internet access. Details regarding the specific effect of specialized services are disclosed to affected customers at the point of sale.

#### **Security Policy**

The Company is dedicated to managing its network to ensure that all customers receive the most secure online experience. We use industry-leading security practices to manage our network, provide services to our customers, and ensure compliance with our Acceptable Use Policy. These tools and practices may change from time to time to keep up with the new and innovative ways that customers use the network and to keep up with changing network technologies.

When malicious behavior is identified, the Company employs various techniques to ensure a positive customer experience. Our security management techniques include ensuring that customer systems are not propagating viruses, or distributing spam email, or engaging in other malicious behavior. We use industry best practices to prevent virus/spam delivery to customer email accounts. We automatically detect and mitigate (Denial of Service) DOS attacks for our customers. We block malicious sites and phishing sites to prevent fraud against our customers and to prevent our customers from getting infected via (Domain Name Service) DNS black-holing and Internet Protocol address (IP) black-holing.

Specific security practices deployed by the Company may include but are not limited to:

**Spoofing Prevention:** The Company applies security measures to prevent an attacker within the network from launching IP spoofing attacks against these machines and flooding the network with unwanted data that can cause congestion.

**DoS/Distributed DoS Monitoring and Mitigation:** The Company applies security measures to prevent an attacker within the network from launching DoS or DDoS to ensure that customers can access the Internet when needed.

Other security practices to address viruses or malware: The Company may also block connections on other ports that are commonly used to exploit other customers or non-customer computers. The Company may also block sites that are used in a malicious manner to infect customers, perform fraud against them and otherwise as needed to protect our network and our customers.

## **Commercial Terms**

Customers can learn about the specific pricing and service availability by calling the customer care number printed on their bills. Customers can access the Company's latest promotional and standard for Broadband Internet Access Service at [www.crosslake.net](http://www.crosslake.net).

The Company's current Broadband Internet Service offering does not include usage-based fees. For full terms and conditions, view Company's Internet Terms and Conditions & Acceptable Use Policy.

The Company may include an early termination fee in the terms of Broadband Internet Access services and promotions offered to customers. The applicability and the extent of an early termination fee may vary depending on the terms of the specific service or promotion purchased by the customer. Customers should reference their Broadband Internet Access Services agreement, promotional advertisements, the terms described in their original order and their order confirmation for details regarding the specific pricing, terms, and the calculation of any early termination fee that may apply to them.

## **Privacy Policy**

Like most companies, we have certain information about our customers and use it to provide our services. We also share it as needed to meet our business goals or fulfill our legal obligations. We protect the information we have about our customers, and we require those we share it with to protect it too. We use information generated on our networks to manage those networks, to plan for future development, and to keep our services running reliably and efficiently. For example, we monitor data to check for viruses, to control spam, to prevent attacks that might disable our services, to ensure that your traffic does not violate our Internet Terms and Conditions & Acceptable Use Policy, and to guard against other inappropriate or illegal activity. This may involve looking at the characteristics of our network traffic, such as traffic volumes, beginning and ending points of transmissions, and the types of applications being used to send traffic across our network. In limited circumstances, we need to examine the content of the data (such as the specific Web sites being visited, files being transmitted, or application being used) for the purposes described above, in circumstances when we are concerned and fraud or harassment, to repair a problem we detect or that a customer contacts us about, or when we are providing the content of broadband traffic to law enforcement which we only do as authorized by law.

## **Redress Policy**

If you have any questions or complaints regarding Crosslake Communications' Broadband Internet Access services and the subjects of this disclosure, you may call the customer care number printed on your bill or send us a message using our <http://www.crosslake.net/contact> page.

Please be sure to include the following information:

- Subject: Broadband Internet Access Service Network Management Disclosure
- A brief summary of the nature of your concern

Crosslake Communications takes all such questions and complaints seriously. The appropriate Company personnel will review all such submissions and respond in a timely manner.