Michigan Broadband Services is committed to providing its customers with the best online experience. We follow industry leading network security standards to ensure the integrity and availability of our broadband network and the confidentiality of our customers' proprietary information. We view network management as critical to the services we provide to our customers. Managing our network well is one of the most important parts of our business. It ensures that our customers have access to the content and applications that they enjoy.

Network Practices

Congestion Management Policy

Michigan Broadband Services monitors and proactively reinforces our network with additional capacity in areas where growth trends identify a need. If acute network congestion occurs, we employ various techniques to ensure a positive customer experience and fair distribution of network resources.

Based on usage history, Michigan Broadband Services customers may encounter congestion, if at all, during the hours of peak usage (7:00 pm and 11:30 pm local time). During peak hours, the majority of residential customers are attempting to use the Internet simultaneously, giving rise to a greater potential for congestion.

Our congestion management techniques include ensuring that customer systems are not propagating viruses or distributing spam email, - i.e. by preventing virus/spam delivery to customer email accounts. We also reinforce our network with additional network capacity in areas where congestion is identified or as part of standard network engineering design plans. In some cases, we may limit the number of customers that may be served on a particular network node until additional capacity can be added. We also seek to ensure that our customers are not excessively using the service. We may contact customers with excessive usage to inquire if it meets with our Acceptable Use Policy.

Application-Specific Policy

Michigan Broadband Services High Speed Internet customers receive full access to all of the lawful content, services, and applications that the Internet has to offer. Michigan Broadband Services does not block, prioritize, or degrade any Internet sourced or destined traffic based on application, source, destination, protocol, or port unless it does so in connection with a security practice described in the security policy section below.

Device Attachment Policy

Customers have the flexibility of attaching any MODEM of their choice to their Michigan Broadband Services High-Speed Internet service provided that the modem supports the technology that the customer is provisioned on. Michigan Broadband Services will not support any MODEM related issues for the customers that attach a non-certified MODEM.

Michigan Broadband Services customers may attach any device of their choice to the MODEM they select.

Michigan Broadband Services also provides a Modem / Wi-Fi routers to customers at no charge. This device provides the technology to attach many customer devices to Michigan Broadband

Services High-Speed Internet service. Additional router equipment is not necessary for most users of the service.

Security Policy

Michigan Broadband Services 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 Internet Terms & Conditions & 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, Michigan Broadband Services 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 Michigan Broadband Services may include but are not limited to:

> IP Spoofing Prevention
>
> The basic protocol for sending data over the Internet network and many other computer networks is Internet Protocol ("IP"). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response.
>
> Michigan Broadband Services 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
>
> A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.
>
> Michigan Broadband Services 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.

Port 25 Blocking

Michigan Broadband Services filters port 25 to reduce the spread of email viruses and spam (unsolicited email). Filtering port 25 has become the industry best practice to reduce the spread of email viruses and spam. These email viruses allow malicious software to control infected computers. These viruses direct the infected machines to send email viruses and spam through port 25. Port 25 filtering is a recognized Internet industry best practice for service providers like Michigan Broadband Services to filter email traffic. The Messaging Anti-Abuse Working Group (MAAWG), a global organization focused on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, recommends that "providers block incoming traffic to your network from port 25."

Read more about MAAWG Port 25 filtering best practices.

Other security practices to address viruses or malware

Michigan Broadband Services may block connections on other ports that are commonly used to exploit other customers or non-customer computers.

Michigan Broadband Services may 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.

In addition to protecting its own network, Michigan Broadband Services provides information to its customers to help them protect themselves when they are online on our Support page.

Performance Characteristics

Service Description Policy

When you order Michigan Broadband Services High-Speed Internet access service, the service we will quote to you is based on the connection speeds that are available at your address. We are continually upgrading our network, but our quoted speed is based on the characteristics of the relevant network facilities at the time you order. We confirm your speed at the time of installation.

The actual speed you experience will vary. During most periods, you can generally expect actual delivered speed ranging from 85% to 100% of the advertised speed purchased. This speed is measured based on the service provided between the outside network interface device and the first equipment where the line connects to. The percentage will vary depending on the amount of bandwidth our network uses in delivering service to you, as well as other factors outside of Michigan Broadband Services facilities control such as customer location, the quality of the inside wiring within the home, the Web sites accessed by the customer, usage of the network during peak periods of the day and the customer's equipment within the premise.

Latency is highly variable depending on the network path, other providers in the path, the actual distance to the destination and performance of the end destinations servers. Michigan Broadband Services High-Speed Internet customers should expect roundtrip latency to most general Internet sites in the range from 50-150ms.

Once service is installed, customers can also determine the throughput of their High-Speed Internet service via Michigan Broadband Services speed test servers available http://speedtest.net.

This website will provide the throughput and latency results for service provisioned over the Michigan Broadband Services network. Third party speed test results may be different than the data provided on the Michigan Broadband Services provided speed test since third party sites may include data for non-Michigan Broadband Services network facilities.

All Michigan Broadband Services High-Speed Internet services are provided either by fiber, or digital subscriber line technology. The particular technology for your service will be based upon what is available in your geographic area. Michigan Broadband Services High-Speed Internet services may be suitable for real-time applications such as VoIP. The suitability for real-time applications depends on the speed purchased, bandwidth required for the application, and time of day usage of the application.

Impact of Specialized Services

Michigan Broadband Services offers video and/or voice specialized services that are carried over the same connection that provides broadband Internet access service. Michigan Broadband Services video services do not negatively affect the performance of the broadband Internet access service. Voice services provided to some small businesses, schools, and libraries may utilize broadband Internet access service capacity to which they subscribe that is otherwise available when voice service is not in use. Details regarding this sharing of capacity between voice and broadband Internet access service are disclosed to these customers at the point of sale.

Commercial Terms

Pricing

Customers can learn about the specific pricing and service availability by calling 1.855.642.4227. Customers can access Michigan Broadband Services latest promotional and standard for High-Speed Internet service at www.michbbs.com.

Customers can also speak with a Michigan Broadband Services representative for services in their area by calling Michigan Broadband Services at 855.642.4227 (Residential) or (Business).

Michigan Broadband Services current High-Speed Internet service offering does not include usage-based fees. For full terms and conditions, view Michigan Broadband Services' Internet Terms & Conditions and Acceptable Use Policy.

Michigan Broadband Services may include an early termination fee in the terms of High-Speed Internet 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 High-Speed Internet Subscriber 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 & Conditions and 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 look into 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 about 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 Options Policy

If you have any questions or complaints regarding Michigan Broadband Services High-Speed Internet services and the subjects of this disclosure, you may call 1.855.642.4227 (Residential) or (Business) or send is a message using our Contact Us page.

Please be sure to include the following information:

- Subject: Internet Management Disclosure
- Your Name: optional
- High Speed Internet Service Address
- A brief summary of the nature of your concern

Michigan Broadband Services takes all such questions and complaints seriously. The appropriate Michigan Broadband Services personnel will review all such submissions and respond in a timely manner.