dishNET Wireline, L.L.C.
High Speed Internet Service Management Policy

dishNET Wireline L.L.C. ("dishNET") strives to provide its customers with excellent high-speed internet service. In order to achieve that goal, dishNET and its vendors work to ensure the confidentiality, integrity and availability of our customer network and of our customers' confidential information. (dishNET and its vendors are collectively referred to as "dishNET".) Managing the performance of the network is an important component of ensuring that customers can access the content and applications they want.

NETWORK PRACTICES

Congestion Management Policy

Based on experience, if customers experience congestion it will be between the peak usage hours of 7:00 p.m. to 11:00 p.m. local time. During those hours, the majority of residential customers are simultaneously attempting to use the Internet which creates a greater potential for congestion.

When network congestion occurs, network engineers will initiate various techniques to maintain a positive customer experience. Those network management techniques include ensuring that customer systems are not propagating viruses or distributing spam email. Additional capacity may be deployed when congestion is identified or is part of a standard network design plan. The number of customers who can access the internet may be limited if a particular network node has limited capacity. dishNET also seeks to ensure that customers are not excessively using the service.

Excessive Use Policy

In order to ensure that an end user does not excessively exceed the data download requirements for their rate plan, your residential service is subject to a data download cap. There is no charge for excessive download usage. dishNET considers variables such as network stability, congestion, availability of customer usage data and the data plan you purchased when analyzing whether to impose a cap on data downloads. The decision to impose a data download cap rests solely with our vendor. When a customer is subject to Excessive Use Policy enforcement, you will receive up to three notices through a mixture of mediums including an online pop-up message, email or telephone call.

If you receive a notice, you must either reduce your internet usage or subscribe to a higher speed residential plan if one is available. This Excessive Use Policy is application neutral and only considers the bytes transferred during a defined period of time independent of protocols, applications or the type of content generating the excessive usage.

Our download guidelines are designed to support today's usage patterns. The updated plans establish the following download limits:

- 1.5Mbps plans – 150 Gigabytes
- Plans greater than 1.5 Mbps – 250 Gigabytes

The median customer usage is about 7 Gigabytes per month with customer downloads ranging between 1 to 30 Gigabytes per month. These usage levels fall significantly below the thresholds of 150 to 250 Gigabytes per month. We estimate that to exceed these guidelines, a customer would have to send, watch, view or listen to: 15 million unique emails; between 300,000 and 500,000 photos; between 40,000 to 80,000 MP3 files; or stream between 1,000 and 3,000 30-minutes shows.

Network usage is generally considered excessive or high volume when a customer uses 30 to 1,000 times the volume of bandwidth compared to other customers in the same speed tier. Less than one-half of a percent of customers (0.5%) approach these limits.

Data that is uploaded to the Internet does not count toward the monthly usage limits. dishNET only uses the downstream direction of the data.

Application-Specific Policy

dishNET customers receive full access to all of the lawful content, services and applications on the Internet. dishNET does not block, prioritize or degrade any Internet sourced or destined traffic based on application, source, destination, protocol or port unless described in the security policy section.

Device Attachment Policy

Customers may attach any Modem of their choice to their dishNET High Speed Internet service provided that the modem complies with dishNET's technical and operational requirements. A determination of the compatibility of customer-owned modems will be

made at the time of ordering the service or you can contact customer support at 855.347.3474.

A customer may attach any device they wish to the modem.

Security Policy

dishNET and its vendors manage the network to ensure all customers receive the most secure online experience. Industry-leading security practices are used to manage our network, provide services to customers and ensure compliance with the dishNET Acceptable Use Policy and High-Speed Internet Agreement. The tools and practices are subject to change without further notice.

When malicious behavior is identified, engineers employ various techniques to ensure a positive customer experience. Security management techniques include ensuring that customer systems are not propagating viruses, or distributing spam email or other malicious behavior. We automatically detect and mitigate (Denial of Service) DOS attacks for our HSI customers. We block malicious sites and phishing sites to prevent fraud against customers and to prevent infections via (Domain Name Service) DNS black-holing and Internet Protocol (IP) Address black-holing.

Specific security practices may include but are not limited to:

IP Spoofing Prevention

Internet Protocol is the basic protocol for transmitting data over the Internet and other computer networks. Each IP packet has a header that contains its numerical source and destination. The packet is normally sent from the sourced address. However, when the header is forged to contain a separate address, the attacker can make it appear the packet was sent from a different machine. When a machine receives the spoofed packets, it sends a response back to the forged source address. dishNET applies security measures to prevent an attacker within the network from launching IP spoofing attacks against 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 designed to make a computer resource unavailable to its users. These attacks are

normally concerted efforts to temporarily or permanently prevent an Internet site or service from functioning. dishNET implements various security measures that prevent an attacker from launching within the network DoS or DdoS attacks to ensure customers can access the Internet.

Port 25 Blocking

dishNET follows industry best practices to reduce the spread of email viruses and spam by filtering port 25. These email viruses allow malicious software to control infected computers by telling the infected machines to send viruses and spam through port 25.

Information on the port 25 filtering best practices established by the Messaging Anti-Abuse Working Group can be reviewed at http://www.uceprotect.net/downloads.MAAWGPort25English.pdf.

Other Security Practices to Address Viruses and Malware

dishNET may block connections on other ports that are commonly used to exploit other customer or non-customer computers. We may block sites that are used in a malicious manner to infect customers, perform fraud against them and as otherwise needed to protect the network and customers.

PERFORMANCE CHARACTERISTICS

Service Description Policy

At the time a customer orders dishNET High Speed Internet Service, the packages we can offer to you will depend upon the connection speeds that are available on the relevant network facilities that reach your address. The advertised is confirmed at the time of installation.

The actual speed you receive will vary. During most periods, you can generally expect the service to perform between 85 to 100 percent of the advertised speed purchased. The speed is measured between the outside network interface device and the first piece of equipment connected to the line. The percentage of advertised speed provided will vary depending upon the amount of bandwidth the network uses in delivering service to you

and other variables. Those factors include your location, the quality of the inside wiring at your premises, the websites accessed, usage of the network during peak periods of the day and the equipment within the premise or home.

Latency within the network varies depending upon on the path the transmission takes through the network, other networks involved in the transmission as well as the actual distance to the destination and performance of servers at the end location. Customers should expect roundtrip latency to most general Internet sites in the range from 50 to 150ms.

COMMERCIAL TERMS

Pricing Policy

dishNET offers its high speed Internet service to residential customers. Customers may purchase dishNET High Speed Internet service with other services by dishNET such as local voice telephone service or satellite television service from its affiliate DISH Network. These services may be combined on one bill and include savings over purchasing standalone services. Availability, features, rates, terms and conditions may vary by location.

Information about specific pricing and service availability can be viewed at www.bundles.dish.com or by calling a sales representative at 1.888.865.5620.

dishNET's High Speed Internet Service does not include usage-based fees. dishNET's Acceptable Use Policy, and High Speed Internet Subscriber Agreement can be found at www.dishnetwireline.com/Policies.

Privacy Policy

Like most companies, dishNET has certain information about customers and uses it to provide services. We share it as needed to meet business goals or to comply with legal requirements. We protect the information we obtain about customers and require vendors and other parties we share the information with to protect it. The information generated on the network is used to manage it, plan future development and keep services running in a reliable and efficient manner. For example, dishNET monitors the network for viruses, to control spam, prevent attacks that might interfere with or disable services, to ensure that

traffic does not violate the subscriber agreement or other policies and to guard against inappropriate or illegal activity. This process may include examining the types of network traffic including volumes, the end points of a transmission and the applications sent across the network. In some circumstances it may be necessary to inspect the content of the data for the purposes described above. Those instances include potential fraud or harassment, to repair a problem that we discover or a customer notifies us about, or when responding to law enforcement when required by law.

The complete Privacy Policy may be viewed at www.dishnetwireline.com/Policies.

Redress Option Policy

If you have a question or complaint about dishNET's High Speed Internet Services and the topics covered by this disclosure, please email us at Regulatory@dishnetwireline.com.

Please include the following information in your email:

- Subject Line: Internet Management Disclosure
- Name: (Optional)
- High Speed Internet Service Address
- A brief summary of the nature of your concern

dishNET will investigate all submissions and respond as soon as possible.

Network vendors

dishNET does not own or operate the network through which you receive your high speed internet access services. Instead, dishNET purchases those services from CenturyLink, an unaffiliated network provider. CenturyLink provides network management services.