

# **Willamette Valley Fiber Network Operations & Copyright Policies**

WVF is committed to providing our customers with the best service experience possible. We use reasonable network management practices that are consistent with industry standards and uses tools and technologies that are minimally intrusive. As Broadband and Telephone services continue to evolve, so too, will our network management policies. We apply reasonable network management practices so our customers are not subject to the negative effects of security attacks, viruses, and spam among other risks resulting in possible degradation of services. You may always access our most current policies at [www.wvalleyfiber.com](http://www.wvalleyfiber.com).

## **Network Overview**

WVF operates a state-of-the-art broadband network whereby fiber optic cable is brought past each home and business. We build a fiber drop from the street to connect to any home or business that purchases services and where access is granted. It should be noted that not all residential apartment buildings and multi-tenant office buildings allow access. The broadband network enables us to bring the benefits of the extraordinary bandwidth carrying capacity of Fiber Optics to each of our customers.

## **Questions, Answers & Information Regarding Our Network Practices**

The FCC requires us to provide descriptions of our Network Management Practices to include Broadband Application-Specific Behavior Practices, Device Attachment Rules, Security Practices, Performance Characteristics, Privacy Policies and Customer Redress Options.

### **Congestion Management:**

Given the current bandwidth capacity no congestion management practice is required nor is a practice being employed today other than network monitoring. We reserve the right to employ congestion management practices in the future.

### **Application-Specific Behavior:**

Does WVF block or rate-control specific protocols?

- We do monitor and prevent certain traffic, such as SPAM, Viruses, BOTs, hackers and other malicious activities, on WVF's internal network. WVF does not do traffic filtering or shaping to the end user (customer). Customers are provided with an open pipe to the internet; all traffic assessment is at their discretion.
- WVF does not assume responsibility for network equipment belonging to the end user, nor their network security practices.
- We do not block any other kinds of traffic. WVF subscribes to the philosophy of complete network neutrality and we treat traffic to and from all customers the same.

Does WVF modify protocol fields in ways not prescribed by protocol standard?

- WVF makes no modification of protocol fields as traffic transits WVF network equipment. WVF adheres to all internet protocol standards.

Does WVF inhibit or favor certain applications or classes of applications?

- We do not inhibit or favor applications or classes of application over our High-Speed Internet/broadband data network. All traffic is treated in a “protocol-agnostic” manner which means management is not based on the applications and is also content neutral.

### **Device Attachment Rules:**

Does WVF have any restrictions on the types of devices that they allow to connect to the network?

- WVF generally allows internet access to any internet capable layer 3 device (i.e. router) with the caveat that each customer is allowed one single public IP address at a time. This restricts the end user to using one single device.

If there are restrictions, is there an approval procedure for devices connecting to the network?

- For any questions regarding the types of devices allowed or required customers should contact WVF’s Sales Department at [csr.WVffiber.net](mailto:csr.WVffiber.net) or at 503 837-0700. While there are no formal approval procedures to get a specific device approved for connection to the network all devices must be UL certified and carry the FCC Part 64 certification.

### **Security:**

What are the practices used to ensure end-user security or security of the network?

- WVF uses the following practices to ensure end-user security and network security:
  - ◊ We employ DHCP Option 82 –This is a protocol that attaches an identifier for all DHCP traffic on the network that identifies what part of the network the traffic originated on and the portion of the network the traffic is trying to reach.
  - ◊ We utilize Anti-Spoof software which is intended to identify and isolate one user’s hardware from impersonating another user’s hardware.
  - ◊ We utilize the industry practice of blacklisting and blocking access from other ISP networks that are spreading malicious software.
  - ◊ The WVF network utilizes encryption as a standard practice on its own internal network. Encryption of traffic generated by, and to and from the end user, is at the users’ discretion. WVF does no traffic modification or additional encryption if the end user chooses to use an unencrypted protocol.
- We utilize these protocols and practices to protect and secure our customer data as well as to protect our broadband network for the benefit of all customers. These protocols allow us to comply with federal CALEA and other Law Enforcement requirements.
- As the Internet evolves so do malware and other types of security exploits. Our security tools and techniques are evolving to meet the security challenges of a 21<sup>st</sup> century world.

- We monitor the network many times per second and a trigger would be finding any instance of unwanted network intrusion on the network. We would react immediately to such an intrusion and would refer to Law Enforcement Agencies as needed.

## **Performance Characteristics**

### Service Description:

A general description of the broadband service offered, including Service Technology, Expected and Actual Speeds, Expected and Actual Latency, Suitability of the Service for Real-time Applications follows:

- Service Technology
  - ◊ WVF uses a FTTH access system to deliver broadband services to customers. The FTTH system standard is called GPON (Gigabit Passive Optical Network). Up to thirty-two (32) customers share one fiber in neighborhoods and this shared fiber is called a PON. The GPON system delivers 2,400 Megabits per second to the subscribers on a PON and 1,200 Mbps from the subscribers on a PON.
  - ◊ In the FTTH network there are no electronics between the substation and the customer. No electronics means that there are fewer failure points in the network and superior service quality to our customers.
- Expected and Actual Speeds
  - ◊ Each subscriber is provided access to two different data products:
    - \* Every data customer is given access to the WVF Intranet. This provides 100 Megabit per second access to and from any other customers on the network. The expected speed for the “Intranet” service is 100 Mbps and the actual speed is 100 Mbps.
    - \* We also offer High Speed Internet access speeds at from 10 Mbps to a Gig. The expected speeds for these products is as advertised and the actual speeds are the same as the advertised. It is possible for customers to experience slower speeds on the open Internet, but slower Internet speeds are due to the nature of the open Internet and not due to any blockage or congestion on the network.
- Expected and Actual Latency
  - ◊ Latency is another measure of Internet performance. Latency is the time delay in transmitting or receiving packets on a network. Latency is primarily a function of the distance between two (2) points of transmission and is typically measured in milliseconds. The network is designed to have an operating latency as great as 20 milliseconds. However, in real practice the actual latency is generally around 3 milliseconds or less.
- Suitability of the Service for Real-time Applications
  - ◊ The network is one of the fastest and most accessible networks available in the U.S. Customers can achieve the speeds on our network that they subscribe to, 24/7, without slowdowns or blockages on our networks.

NOTE: latency may be disclosed using either the median latency or a range of actual latencies that includes the median latency. If speed or latency ranges are used, the percentiles used to determine the endpoints of the ranges must also be disclosed.

## **Impact of Specialized Services:**

What specialized services, if any, are offered to end users?

- WVF offers one service that could be considered a “Specialized” service over the access system. That service is IP Video (IPTV).
- Both IP Video is delivered to customers over a different data segment than the one used for broadband data traffic (including High Speed Internet traffic) and never affects a customer’s access to the WVF Intranet or the open Internet.

Do any of these specialized services affect the last mile capacity available for, and performance of broadband internet access service?

- Under no circumstances does IP Video affect the performance of the Broadband services.

## **Privacy Policies:**

Do network management practices entail inspection of network traffic?

We examine traffic to the extent needed to utilize the network safety features listed earlier such as eliminating spam or intercepting malware which may be a direct threat to the WVF NOC internal network. We do not inspect or filter any customer traffic for any purpose other than to keep track, at the network level, where traffic flows in order to make certain that the network is adequate for the demands of customers.

Is traffic information stored, provided to 3<sup>rd</sup> parties or used by the ISP for non-network management purposes?

The only time that any stored information is provided to any 3<sup>rd</sup> party is in response to a court order from a valid and qualified Law Enforcement Agency.

## **Redress Options:**

What are WVF’s practices for resolving end-user and edge provider complaints and questions?

First, we log all complaints of trouble as a trouble ticket in a trouble log system. This allows for a numeric identification of each trouble reported on the network. Trouble tickets can be generated by customers or self-generated by alarms located on the network.

Secondly, we assign a priority to each trouble ticket based upon the perceived severity of the problem. For example, outages involving multiple customers are given a higher priority than a minor network glitch affecting one customer.

We attempt to identify and address problems from its Network Operations Center (NOC). If the NOC is unable to clear a reported problem, then a technician in a truck is dispatched to address the problem.

If the problem is of such severity that a field technician cannot solve the problem, the problem is escalated to an engineer. If the engineer is unable to solve the problem, it is generally escalated to an external engineer or consultant or to the vendor that made the

equipment in question. WVF contracts with experienced vendors for as needed troubleshooting and resolution in support of the network.

Finally, the customer may be notified depending upon the severity and type of problem.

Trouble tickets are retained permanently so that WVF is able to view a history of trouble at a specific customer site, a specific neighborhood or with a specific brand or piece of equipment.

### **Prohibited Uses and Activities**

Our Customer Service Agreement prohibits uses and activities of the service that interfere with or diminish the use and enjoyment of the service by others, infringe on the rights of others or that are illegal. These prohibited uses and activities are listed below and include, but are not limited to, using the service, the customer equipment or the WVF equipment either individually or in combination with the other, to:

- undertake or accomplish any unlawful purpose which includes, but is not limited to, posting, storing, transmitting or disseminating data, information or materials which are unlawful, libelous, obscene, defamatory, threatening or which infringe on the intellectual property rights of any person or entity in any way that would constitute or encourage conduct that would constitute a criminal offense or violate any local, state, federal or international law, order or regulation;
- upload, post, transmit, publish, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner;
- transmit unsolicited commercial or bulk messages commonly know as “spam”;
- participate in the collection of very large numbers of e-mail addresses, screen names, or other identifiers of others without their prior consent, participate in the use of software designed to facilitate these activities, i.e. “harvesting” or collect responses from unsolicited bulk messages;
- falsify, alter, or remove message headers;
- falsify references to WVF or its network, by name or any other identifier, in messages;
- impersonate any person or entity, or forge any person’s digital or manual signature;
- engage in sender address falsification, often know as “phishing”;
- violate the terms of service of any network, server, application, or Web site that you access or use;
- posting or transmitting any information or software which contains a worm, virus or other harmful feature regardless of intent, purpose or knowledge;
- utilize or distribute devices designed or used to compromise security or whose use is otherwise unauthorized including but not limited to password guessing programs, decoders, keystroke loggers, packet sniffers, encryption circumvention devices and Trojan Horse programs;
- engage in port scanning;
- utilize or run Web hosting, file sharing or proxy services and servers or other dedicated, stand-alone equipment, or servers from the premises that provides service, including network content, to any party outside your premises local area network;

- utilize or run programs from the premises that provides service, including network content, to any party outside your premises local area network, except for personal and non-commercial use;
- copy, distribute, or sublicense any proprietary software provided by WVF or any third party in connection with the Service, except that one copy of each software program may be made by the customer for back up purposes only;
- disrupt or cause a performance degradation to the service or any WVF facilities or equipment used to deliver the service regardless of intent, purpose or knowledge;
- alter/modify, or tamper with WVF equipment or permit any other party, not authorized by WVF, to do same including connecting WVF equipment to any computer outside of your premises
- resell the Service in whole or in part, directly or indirectly.

### **Treatment of Personal Web Pages and File Storage**

Customers and users are solely responsible for any and all information published or stored on Personal Web Pages and/or File Storage and for ensuring that all content is appropriate for those who may have access to it. This includes taking appropriate measures and precautions to prevent minors from accessing or receiving inappropriate content. This includes, but is not limited to, text, photographs, logos, executable programs, video and audio recordings, images, and illustrations. WVF reserves the right to remove or block content contained on Personal Web Pages/File Storage if we, in our sole discretion, determines that it violates the terms of this Acceptable Use Policy.

### **Treatment of Inappropriate Content and Transmission**

We reserve the right to refuse to transmit or post, and remove or block, any information or materials, in whole or in part, that we, in our sole discretion, deems to be in violation of WVF policies. While we have no obligation to monitor transmissions or postings made on the service we have the right to monitor these transmission and postings for violations of WVF policy and to disclose, block, or remove them in adherence with the Master Service Agreement, and applicable law.

To report a violation contact WVF at 503-837-1700, or [www.wvalleyfiber.com](http://www.wvalleyfiber.com). To report a child exploitation incident involving the Internet, report to the same contacts noted above.

### **Copyright and Digital Millennium Copyright Act Requirements**

WVF has procedures in place dedicated to compliance with U.S copyright laws and requires all customers and users of the service to comply with these laws. In compliance with these laws and WVF policy you may not store any material or content on, or disseminate any material or content over, the service in any manner that constitutes an infringement of third-party intellectual property rights. This includes rights granted by U.S. copyright law. In accordance with the Digital Millennium Copyright Act of 1998 WVF reserves the right to terminate the service provided to any customer or user who is found to have violated third party copyright or other intellectual property rights.

Alleged infringement of copyrighted material and content stored on the service may be reported by the copyright owner, in compliance with the DMCA notification requirements, with WVF's

authorized agent at the address below:

Chad Stokes, Attorney  
Cable Huston  
1001 SW 5<sup>th</sup>, Suite 2000  
Portland, OR 97204

All notifications must comply with the requirements of Section 512(c)(3) of the U.S. Copyright Act. Upon receipt of a compliant notification we will directly or indirectly remove the allegedly infringing work(s) stored on the service or will disable access to the work(s). All affected customer(s) or user(s) of the service will be notified of the removal or disabling.

Should you receive a notification of alleged infringement and you believe in good faith that the allegedly infringing works have been removed or blocked by mistake you may file a counter notification, in adherence with Section 512(g)(3) of the U.S. Copyright Act, to the address listed above. We will adhere to DMCA procedure and will provide a copy to the party that filed the original notification. In doing so, the WVF will be held harmless and will not be made a party to any dispute or lawsuit resulting from or in association with the alleged copyright infringement.

**WVF reserves the right to modify this document at any time. We will notify you of any material changes via written, electronic, or other means permitted by law, including by posting it on our website. If you find the changes unacceptable, you have the right to cancel the Services. If you continue to use the Services after receiving notice of such changes, we will consider that as your acceptance of the changes.**

**Version Update: 6/29/2020**