TVIfiber
TALLAHATCHIE VALLEY INTERNET SERVICES

Tallahatchie Valley Internet Services

P.O. Box 512 Batesville, Mississippi 38606
(662) 563-2075

Network Management Policy

Tallahatchie Valley Internet Services dba TVIFiber is committed to providing our customers with the best online experience possible. TVIFIBER uses reasonable network management practices that are consistent with industry standards and uses tools and technologies that are minimally intrusive. Just as the Internet continues to evolve, so too, will our network management policies. Should TVIFIBER not apply reasonable network management practices our customers could be subject to the negative effects of security attacks, viruses, and spam among other risks resulting in possible degradation of services. You may also access our most current Acceptable Use Policy (AUP) at https://tvifiber.com.

Network Overview

TVIFIBER operates a state-of-the-art broadband network whereby fiber optic cable is brought past each home and business. TVIFIBER builds a fiber drop from the street to connect to any home or business who 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 TVIFIBER's customers.

Questions, Answers & Information Regarding Our Network Practices

The FCC requires us to provide descriptions of our Network Management Practices to include 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. TVIFIBER reserves the right to employ congestion management practices in the future.

Application-Specific Behavior:

Does TVIFIBER block or rate-control specific protocols?

- TVIFIBER does block certain traffic to protect TVIFIBER broadband customers from malicious applications such as SPAM, Viruses, BOTs, hackers and other malicious activities. TVIFIBER blocks traffic from network sources that are known by the industry to spread malware and from applications that are known to propagate these malicious activities.
- If TVIFIBER did not block and/or control these types of activities, TVIFIBER high speed Internet customers' end devices could become

infected with viruses and other malware that could in-turn affect other networks through the Internet.

- TVIFIBER does not block any other traffic. TVIFIBER subscribes to the philosophy of complete network neutrality and treats traffic to and from all customers the same.

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

- TVIFIBER does not modify protocol fields not prescribed by protocol standards.

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

- TVIFIBER does not inhibit or favor applications or classes of application over its 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 TVIFIBER have any restrictions on the types of devices that they allow to connect to the network?

- TVIFIBER does not allow customers to connect switches or hubs directly to the IP port. A customer is limited to one (1) mac address per service port.

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 info@tvifiber.com. 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?

- TVIFIBER uses the following practices to ensure end-user security and network security:
  - TVIFIBER employs S-Flow –This is a protocol that attaches an identifier for all traffic on the network. S-Flow captures the source and destination of all traffic allowing TVIFIBER to properly engineer and troubleshoot the network.
  - TVIFIBER implements DDOS mitigation software which blocks malicious attacks that intended to disrupt service from the internet to TVIFIBER's network.
  - TVIFIBER utilizes Anti-Spoof software which is intended to identify and isolate one user's hardware from impersonating another user's hardware.
  - TVIFIBER utilizes the industry practice of blacklisting and blocking access from other ISP networks that are spreading malicious software.

        - The TVIFIBER network utilizes encryption and the data from every customer is encrypted to stop unlawful access to specific traffic.
    - TVIFIBER utilizes these protocols and practices to protect and secure TVIFIBER customer data as well as protect the TVIFIBER broadband network for the benefit of all customers. These protocols allow TVIFIBER to comply with federal CALEA and other Law Enforcement requirements.

What conditions trigger a security mechanism to be invoked?

- The encryption protocols and practices used on the TVIFIBER fiber network provide far more security than is available with other technologies.
- As the Internet evolves so do malware and other security exploits. TVIFIBER's security tools and techniques are evolving to meet the security challenges of a 21st century world.
- TVIFIBER continually monitors the network. In the event of a security breach, an alarm would trigger. TVIFiber will react immediately to the network intrusion and will refer to Law Enforcement Agencies as need.

Performance Characteristics:

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

- Service Technology
    - TVIFIBER 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 (downstream) and 1,200 Mbps from the subscribers on a PON (upstream).
    - In the TVIFIBER FTTH network there are no electronics between the Central Office (CO) and the customer. No electronics equates to fewer failure points in the network resulting in superior service quality to our customers.

- Expected and Actual Speeds
    - Each subscriber is provided access to two different data products:
        - TVIFIBER offers a symmetrical 300Mbps High Speed Internet service. This service offering provides 300Mbps download and upload speeds. The expected speed for this service is 300Mbps download and upload.
        - TVIFIBER also offers a symmetrical 1Gbps High Speed Internet service. 1Gbps equates to 1000Mbps download and upload. The expected speed for this service is 1000Mbps download and upload. 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 TVIFIBER 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 TVIFIBER network is designed to have an operating latency as great as 30 milliseconds. However, in real practice the actual latency is generally around 20 milliseconds or less.

- Suitability of the Service for Real-time Applications
  - The TVIFIBER 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.

System and Network Security

Users are prohibited from violating or attempting to violate the security of TVIFIBER, including, without limitation, (a) accessing data not intended for such User or logging into a server or account which such User is not authorized to access, (b) attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorization, (c) attempting to interfere with, disrupt or disable service to any user, host or network, including, without limitation, via means of overloading, flooding, mail bombing or crashing, (d) forging any packet header or any part of the header information in any E-mail or newsgroup posting, or (e) taking any action in order to obtain services to which such User is not entitled. Violations of system or network security may result in civil or criminal liability. We may investigate occurrences that may involve such violations, and we may involve and cooperate with law enforcement authorities in prosecuting Users who are alleged to be involved in such violations.

Suspension or Termination

Any User which TVIFIBER determines, in its sole discretion, to have violated any element of this Network Management Policy shall receive a written warning, and may be subject at our discretion to a temporary suspension of service pending such User's agreement in writing to refrain from any further violations; provided that TVIFIBER may immediately suspend or terminate such User's service without issuing such a warning if TVIFIBER, in its sole discretion deems such action necessary. If we determine that a User has committed a second violation of any element of this Network Management Policy, such User shall be subject to immediate suspension or termination of service without further notice, and we may take such further action as we determine to be appropriate under the circumstances to eliminate or preclude such violation. TVIFIBER shall not be liable for any damages of any nature suffered by any customer, User, or any third party resulting in whole or in part from TVIFIBER exercise of its rights under this Policy. Additional requirements and/or penalties apply as found in TVIFIBER's Acceptable Use Policy (AUP).

Service Monitoring

TVIFIBER has no obligation to monitor the services but may do so and disclose information regarding the use of the services for any reason if we, in our sole discretion, believe that it is reasonable to do so, including to satisfy laws, regulations, or other governmental or legal requirements or requests; to operate the services properly, or to protect itself and its subscribers.

Privacy

Any User interacting with our site and providing TVIFIBER with, address, telephone number, E-mail address, domain name or URL or any other personally identifiable information permits TVIFIBER to use such information for commercial purposes of its own, including contacting Users about products and services which may be of interest. All information concerning our users shall be kept in accordance with the TVIFIBER then-applicable Privacy Policy and the requirements of applicable law.

Impact of Specialized Services

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

- TVIFIBER offers one service that could be considered "Specialized" services over the access system. This service is IP Telephone Service (VoIP).
- IP VoIP 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 TVIFIBER 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 VoIP affect the performance of the Broadband services.

Network Inspection

Do network management practices entail inspection of network traffic?

TVIFIBER examines traffic to the extent needed to utilize the network safety features listed earlier such as eliminating spam or intercepting malware. TVIFIBER does not inspect traffic for any other purposes other than to keep track, at the network level, where traffic flows ensuring that the network is adequate for the demands of customers.

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

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

Complaint Redress Options

What are TVIFIBER's practices for resolving end-user and edge provider complaints and questions?

TVIFIBER first logs 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 TVIFIBER network.

Secondly, TVIFIBER assigns 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 issue affecting one customer.

TVIFIBER attempts 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. TVIFIBER has established maintenance and support contract with experienced vendors for 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 TVIFIBER can 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

TVIFIBER's Acceptable Use Policy (AUP) 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 TVIFIBER 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 TVIFIBERs, 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 TVIFIBER or its network, by TVIFIBER 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, keystoke 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 TVIFIBER 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 TVIFIBER facilities or equipment used to deliver the service regardless of intent, purpose or knowledge;
▪ alter/modify, or tamper with TVIFIBER equipment or permit any other party, not authorized by TVIFIBER, to do same including connecting TVIFIBER 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. TVIFIBER reserves the right to remove or block content contained on Personal Web Pages/File Storage if TVIFIBER, in its sole discretion, determines that it violates the terms of this Acceptable Use Policy.

Treatment of Inappropriate Content and Transmission

TVIFIBER reserves the right to refuse to transmit or post, and remove or block, any information or materials, in whole or in part, that TVIFIBER, in its sole discretion, deems to be in violation of our posted Policies. While TVIFIBER has no obligation to monitor transmissions or postings made on the service TVIFIBER has the right to monitor these transmission and postings for violations of TVIFIBER Policies and to disclose, block, or remove them in adherence with our Customer Service Agreement and our Acceptable Use Policy (AUP), and applicable law.
To report a violation, contact dmca@tvifiber.com. To report a child exploitation incident involving the Internet, contact CALEA_Request@tvifiber.com.

No Waiver/Severability

Any failure of TVIFIBER to enforce this Policy shall not be construed as a waiver of any right to do so at any time. If any portion of this Policy is held invalid or unenforceable, that portion will be construed consistent with applicable law, and any remaining portions will remain in full force and effect.

TVIFIBER reserves the right to modify this Network Management Policy 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.

Effective May 18, 2023