Terabit Networks provides Broadband Internet Access Service on a best effort, month-to-month basis. Customers can cancel service at any time with no early termination fee. Equipment supplied by Terabit must be returned upon termination of service, or customer agrees to pay replacement cost. Customer agrees that Terabit is not liable for consequential damages (e.g. you lose an eBay auction or a securities trade because of an outage) or the actions of third parties (e.g. you fall for an online scam). If you depend on the internet for your livelihood, you should invest in a secondary service for backup. Again, there is no implied or express service level agreement with this service. It is a simple best effort. It will go down from time to time.

Service includes maintenance of network equipment, which remains the property of Terabit, up to and including the Power Over Ethernet adapter (or Voice over IP adapter if customer has Digital Phone service). Customer is responsible for local area network equipment such as wireless routers, computers, printers, video devices, game consoles, tablets and smartphones.

Our Terms of Service may change from time to time, in which case the current version will be posted on our website. Continued use of the service constitutes agreement to these terms. If at any time you feel that you cannot follow these Terms or the Acceptable Use Policy, you are advised to stop using the service and call our office to cancel and receive a refund for any prepaid service.

Acceptable Use Policy

Terabit accounts may not be used for activities which are illegal or harmful to other Internet users or networks, including (but not limited to) activities listed below. Terabit may filter, suspend or terminate accounts as necessary to stop such activities.

1. Sending unsolicited bulk email a.k.a "spam".
2. Hosting an "open mail relay" (open to spammers to relay mail).
3. Hosting any application that is seeding torrents or other distributed storage methods that use your connection to store cloud based data for others.
4. Attempts to break into other computers or networks including hacking, portscanning, rootkits, trojans, session hijacking, etc.
5. Denial of service attacks (including use of booter sites against other gamers).
6. Intentionally transmitting malware.
7. Faking IP addresses or email headers for malicious or fraudulent purposes.
8. Transmitting, posting on a website, or sharing via P2P networks any of the following - bootleg software a.k.a. "warez", pornography, or hate literature.
9. Transmitting, posting or sharing copyrighted material without the approval of the copyright holder (see DMCA policy below).
10. Libel or slander.
11. Attempts to obtain products or services fraudulently.

Customer is responsible for insuring that others with access to the service follow these rules. Service is not for resale or sharing without written authorization from Terabit. WiFi routers must be secured with a password and not open for use by the general public. Any WiFi sharing will result in immediate termination of the account with no refund of the installation fee.

WiFi sharing is not only an illegal theft of service but it opens one to becoming an accomplice or accessory to criminal actions done by others.

Internet services are provided on a best-effort basis. Outages or performance degradation can occur due to circumstances beyond our control, and we cannot be held responsible for consequential damages. Our liability is limited at most to a prorated refund. Services are not intended for "high risk use" where interruption of service can result in personal injury or damage to property. Residential internet usage is historically aperiodic and bursty. We count on the historic bursty nature to calculate the needs of our backbone. Internet backbone capacity is designed to statistically have overhead at all times for the needs of all customers. This works well for networks with large numbers of users. At this point in time (3/29/2021) Terabit Networks has a low number of customers so that if all the customers tried to use their maximum bandwidth at the same time, some backbone congestion will occur. If we discover a customer is using maximum capacity a large portion of the time we will discuss the problem with the customer but we do reserve the right to throttle, limit or disconnect the customer until a technical solution can be created.

Access to the Internet includes access to offensive material, spam, viruses, hackers, vice, get-rich-quick schemes, hoaxes and fraud. Even though we may offer services like spam and virus filtering, they are not foolproof. We just provide the connection to the Internet, you are responsible for how you use that connection. We cannot take responsibility if you are offended, cheated, infected or hacked by third parties on the Internet.

Redress

Customers experiencing problems with their service should call our office at XXX-XXX-XXXX. If our office is closed or all support techs are busy, please leave a voicemail message with your callback number and a description of the problem. If you feel your problem has not been adequately addressed, please ask for escalation to a manager.

Service is month-to-month and customers can cancel service at any time without paying an early termination fee.

Customers should contact us and give us a reasonable chance to resolve technical or billing issues before seeking other forms of redress such as complaining to regulatory agencies or taking legal action. Compensation for outages will be limited to a prorated refund, we are not responsibile for consequential damages. Customers who need Internet access for mission critical use are advised to have a backup access method such as a mobile hotspot.

Open Internet Policy

Terabit supports Open Internet principles. We do not block access to legal content on the Internet. We do not throttle or prioritize traffic for business reasons, although we may engage in reasonable network management for technical reasons or to protect the network from attack as authorized by the FCC (see Network Management Policy below).

Note that we may block certain traffic for security reasons. We block packets destined to TCP ports 135, 137-139 and 445 which are for Windows LAN traffic and are not intended to propagate onto wide area networks. Packets to port 25 may be blocked to deal with spam issues. Packets from spoofed source addresses or to bogus destination addresses known as "bogons" may be blocked. We may also need to block malicious traffic in order to deal with amplification or denial of service attacks.

FCC Notice

If a customer believes this Open Internet Policy is not in compliance with FCC regulations, the customer may file an informal complaint at the Federal Communications Commission. The FCC urges customers to submit any complaints via its website at the following address:

http://esupport.fcc.gov/complaints.htm.

Customers may also file a formal complaint at the FCC using Part 76 of the Commission's rules.

Network Management Policy

Congestion may occur when a customer tries to send or receive more traffic than the speed plan they are subscribed to. A lot of traffic (e.g. software updates, email, cloud backup, video previews) happens automatically. Video streaming services try to determine the available connection speed and use 100% of it. With multiple users in a household, it is inevitable that the amount of traffic will sometimes exceed the subscribed connection speed. If this happens constantly, the customer may need to upgrade to a faster tier of service.

Device Attachment Policy

Routers will need to have a WAN (Internet) port capable of 10/100 Ethernet and must support DHCP and PPPoE Internet connection types. WiFi must be secured with a password. If router remote management is enabled, it must be secured with a non-default administrative password.

Privacy Policy

We do not monitor any customer traffic or log or save any information about what customers are doing with the internet. We do monitor usage levels but not content.

We do not use customer contact information or Internet browsing habits for marketing purposes, and we do not share or sell this information with third parties. We do not modify webpages or DNS lookups to insert ads, and we do not modify headers to allow advertisers to track you. This may seem obvious, but many ISPs do these things to enhance their revenue.

In rare circumstances, customer information may be requested by a law enforcement agency (LEA), and we will comply if presented with a valid subpoena, court order or national security letter. We reserve the right to make an exception if lives are in imminent danger, e.g. a hostage or suicide crisis.

Theoretically we could be ordered to provide the equivalent of a wiretap under the CALEA Act. Any information provided will be restricted to the scope of the court order and avoid revealing information about any other customer.

As discussed below under DMCA Policy, we do not hand out customer information just because a copyright holder or their lawyers submit a notice of claimed infringement. They would have to obtain a valid subpoena or court order.

Customer Proprietary Network Information (CPNI) Policy

We will need to verify that you are the account holder before discussing or changing your services or passwords. If you want someone else like a family member or computer technician to have access to this kind of information, we may need to obtain your authorization.

Digital Millennium Copyright Act (DMCA) Policy

If we receive a DMCA Notice of Claimed Infringement from a copyright holder, our policy is to make a reasonable effort to forward the notice to the customer who was using the stated IP address at the stated time. We do not disclose any customer information unless served with a subpoena or court order. In the case of frequent or repeated notices involving the same customer, we may warn the customer to cease any activities that violate the DMCA (these cases typically involve peer to peer filesharing). If we continue to receive notices of copyright infringement, we are required by the DMCA to have a repeat infringer policy, which may lead to suspension of service or termination of the account.

(last updated 3/29/2021)

For more information, please call 435-465-1012 or email sales@terabit.com.