Network Management Policy

Cimplenet/Ultranet LLC is committed to providing our Subscribers with the best online experience possible. We use reasonable network management practices consistent with industry standards and use minimally invasive tools and technologies. Just as the Internet continues to evolve, so too, will our network management policies. Should Cimplenet/Ultranet LLC not apply reasonable network management practices, our Subscribers could be subject to the negative effects of, among other risks, security attacks, viruses, and spam, resulting in possible degradation of services. All though Cimplenet and its providers work hard to protect its customers this is never guaranteed 100%, any and all Internet users should maintain and update devices, virus protection and use caution when using the Internet from any provider as there is always some threat during its use as the Internet is a public domain and is subject to any and all traffic good and bad.

Network Overview

Cimplenet/Ultranet LLC operates a mixture of Wireless and Wired broadband networks whereby fiber is provided by local providers to our tower and pole locations. Cimplenet/Ultranet LLC builds out a wireless infrastructure to reach homes and businesses that purchase services and where access is granted. (It should be noted that not all residential apartment buildings and multi-tenant office buildings allow access.) This wireless network enables us to bring the benefits of High Speed Internet to locations other ISP's may be unable to reach.

Our Network Practices

The FCC requires us to provide descriptions of our Network Management Practices to include Security Practices, Performance Characteristics, and Privacy Policies.

Congestion Management:

Given the current bandwidth capacity, no congestion management practice is required nor is a practice being employed today other than network monitoring. Cimplenet/Ultranet LLC reserves the right to employ congestion management practices in the future.

Application-Specific Behavior:

Does Cimplenet/Ultranet LLC block or rate-control specific protocols?

- Cimplenet/Ultranet LLC or its providers block certain traffic to protect Cimplenet/ Ultranet LLC broadband Subscribers from malicious applications such as spam, viruses, bots, hackers and other malicious activities. Cimplenet/Ultranet LLC or its provider blocks traffic network sources that are known by the industry to spread malware and from applications that are known to propagate these malicious activities.

- If Cimplenet/Ultranet LLC did not block and/or control these types of activities, Cimplenet/Ultranet LLC high speed Internet Subscribers' computers could become infected with all manner of viruses and other malware that could in-turn affect other networks through the Internet.
- Cimplenet/Ultranet LLC does not block any other kinds of traffic. Cimplenet/Ultranet LLC subscribes to the philosophy of complete network neutrality, and we treat traffic to and from all Subscribers the same.

Does Cimplenet/Ultranet LLC modify protocol fields in ways not prescribed by protocol standard?

- Cimplenet/Ultranet LLC does not modify protocol fields not prescribed by protocol standards.

Does Cimplenet/Ultranet LLC inhibit or favor certain applications or classes of applications?

- Cimplenet/Ultranet LLC 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 Cimplenet/Ultranet LLC restrict the types of devices that it allows to connect to the network?

- Cimplenet/Ultranet LLC does not allow Subscribers to connect switches or hubs directly to the IP port. A customer is limited to one (1) MAC address per service port.

Is there an approval procedure for devices connecting to the network?

- For any questions regarding the types of devices allowed or required, Subscribers should contact Customer Service. 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.

Performance Characteristics:

- Expected and Actual Speeds ○ The expected speeds for our products are as advertised and the actual speeds are the same as advertised. However, it is possible for Subscribers 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 Cimplenet/ Ultranet LLC 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 39 milliseconds. However, in real practice, the actual latency is generally around 6 milliseconds or less.

System and Network Security

Users are prohibited from violating or attempting to violate the security of Cimplenet/Ultranet LLC, 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, email bombing or crashing, (d) forging any packet header or any part of the header information in any Email 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 Subscriber, User or Third-Party (collectively "User") which Cimplenet/Ultranet LLC 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 Cimplenet/Ultranet LLC may immediately suspend or terminate such User's service without issuing such a warning if Cimplenet/Ultranet LLC, 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. Cimplenet/Ultranet LLC shall not be liable for any damage of any nature suffered by any Subscriber, User, or any third party resulting in whole or in part from Cimplenet/Ultranet LLC exercise of its rights under this Policy. Additional requirements and/or penalties apply as found in Cimplenet's Acceptable Use Policy (AUP).

Service Monitoring

Cimplenet/Ultranet LLC has no obligation to monitor the services and does not do so on a day to day bases 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.

Any User interacting with our site and providing Cimplenet/Ultranet LLC with address, telephone number, email address, domain name or URL, or any other personally identifiable information permits Cimplenet/Ultranet LLC 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 Cimplenet/Ultranet LLC then-applicable Privacy Policy and the requirements of applicable law.

Prohibited Uses and Activities

Our posted 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 again listed below in detail and include, but are not limited to, using the service, the Subscriber equipment, or the Cimplenet/ Ultranet LLC 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 known as “spam”;
- participate in the collection of very large numbers of email addresses, scanning Cimplenet/Ultranet LLC’s, 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 Cimplenet/Ultranet LLC or its network, by Cimplenet/Ultranet LLC 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 known 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 Cimplenet/Ultranet LLC 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 Cimplenet/Ultranet LLC facilities or equipment used to deliver the service regardless of intent, purpose or knowledge;
- alter/modify, or tamper with Cimplenet/Ultranet LLC equipment or permit any other party, not authorized by Cimplenet/Ultranet LLC, to do same including connecting Cimplenet/Ultranet LLC equipment to any computer outside of your premises; or
- resell the Service in whole or in part, directly or indirectly.

Treatment of Personal Web Pages and File Storage

Subscribers and users are solely responsible for 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.

Treatment of Inappropriate Content and Transmission

Cimplenet/Ultranet LLC reserves the right to refuse to transmit or post, and remove or block, any information or materials, in whole or in part, that Cimplenet/Ultranet LLC, in its sole discretion, deems to be in violation of our posted Policies. While Cimplenet/Ultranet LLC has no obligation to monitor transmissions or postings made on the service Cimplenet/Ultranet LLC has the right to monitor these transmission and postings for violations of Cimplenet/Ultranet LLC Policies and to disclose, block, or remove them in adherence with our Customer Service Agreement, our Acceptable Use Policy (AUP), our Cybersecurity Policy and applicable law.

No Waiver/Severability

Any failure of Cimplenet/Ultranet LLC 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.

Cimplenet/Ultranet LLC 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 1, 2024