North Alabama Electric Cooperative
Network Management Policy

North Alabama Electric Cooperative ("NAEC" or "Company") is committed to providing our customers with the best online experience possible. NAEC uses reasonable network management practices consistent with industry standards and uses minimally invasive tools and technologies. Just as the Internet continues to evolve, so too will our network management policies. Should NAEC not apply reasonable network management practices, our customers could be subject to the negative effects of, among other risks, security attacks, viruses, and spam, resulting in possible degradation of services. You may also access our most current Acceptable Use Policy (AUP) on our website, naecoop.com.

Network Overview

NAEC operates a state-of-the-art broadband network whereby fiber optic cable is brought past each home and business. NAEC builds 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 NAEC subscriber.

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. NAEC reserves the right to employ congestion management practices in the future.

Application-Specific Behavior:

Does NAEC block or rate-control specific protocols?

- NAEC blocks certain traffic to protect NAEC broadband subscribers from malicious applications such as spam, viruses, bots, hackers, and other malicious activities. NAEC blocks traffic network sources known by the industry to spread malware and from applications known to propagate these malicious activities.
- If NAEC did not block and/or control these types of activities, NAEC 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.
- NAEC does not block any other kinds of traffic. NAEC applies the philosophy of complete network neutrality, and we treat traffic to and from all subscribers the same.

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

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

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

- NAEC 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 NAEC restrict the types of devices that it allows to connect to the network?

- NAEC 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, 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.

Security:

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

- NAEC uses the following practices to ensure end-user security and network security:
    - NAEC employs protocols that can identify traffic on the network, what part of the network the traffic originated on, and what portion of the network the traffic is trying to reach. These protocols help NAEC understand the flow of network traffic to best engineer the network and troubleshoot it.
    - NAEC utilizes anti-spoof software which is intended to identify and isolate one user's hardware from impersonating another user's hardware.
    - NAEC utilizes the industry practice of blacklisting and blocking access from other ISP networks that are spreading malicious software.
    - The NAEC network utilizes encryption to stop unlawful access to specific traffic.
- NAEC utilizes protocols and practices to protect and secure subscriber data as well as to protect the NAEC broadband network for the benefit of all subscribers. These protocols allow NAEC to comply with federal CALEA and other Law Enforcement requirements.

What conditions trigger a security mechanism to be invoked?

- NAEC monitors the network many times per second, and a trigger would be finding any instance of unwanted network intrusion on the network. NAEC would

react immediately to such an intrusion and would refer to Law Enforcement Agencies as needed.

Performance Characteristics:

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
  - NAEC uses a FTTH access system to deliver broadband services to customers.
  - In the NAEC network, there are no electronics between the fiber hut and the customer. No electronics means that there are fewer failure points in the network and superior service quality for our customers.
- Expected and Actual Speeds
  - The expected speeds for our products are at the advertised rates, and the actual speeds are within a reasonable variance as advertised. Customers may experience slower speeds on the open Internet due to the open Internet and not due to any blockage or congestion on the NAEC 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 NAEC network is designed so that the actual latency is generally around 20 milliseconds or less.
- Suitability of the Service for Real-time Applications
  - 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:

Subscriber and/or Users are prohibited from violating or attempting to violate the security of NAEC, including, without limitation, (a) accessing data not intended for such Subscriber and/or User or logging into a server or account which such Subscriber and/or 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 email or newsgroup posting, or (e) taking any action to obtain services to which such Subscriber and/or User is not entitled. Violations of system or network security may result in civil or criminal liability. We may investigate occurrences involving such violations, and we may involve and cooperate with law enforcement authorities in prosecuting Users who are alleged to be involved in such violations. Additional requirements and/or penalties apply as found in NAEC's Acceptable Use Policy (AUP).

Suspension or Termination:

Any Subscriber or User which NAEC 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 Subscriber's agreement in writing to refrain from any further violations; provided that NAEC may immediately suspend or terminate such User's service without issuing such a warning if NAEC, in its sole discretion deems such action necessary. If we determine that a Subscriber or User has committed a second violation of any element of this Network Management Policy, such Subscriber or 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. NAEC shall not be liable for any damages of any nature suffered by any Subscriber, customer, User, or any third party resulting in whole or in part from NAEC's exercise of its rights under this Policy. Additional requirements and/or penalties apply as found in NAEC's AUP.

Service Monitoring:

NAEC 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.

Network Inspection:

Do network management practices entail inspection of network traffic?

- NAEC examines traffic to the extent needed to utilize the network safety features listed earlier such as eliminating spam or intercepting malware. NAEC does not inspect 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 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 NAEC's practices for resolving end-user and edge-provider complaints and questions?

- NAEC first logs all complaints of trouble as a trouble ticket in a trouble log system. This allows for numeric identification of each trouble reported on the network.

- NAEC assigns a priority to each trouble ticket based upon the perceived severity of the problem.
- NAEC 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. NAEC contracts with experienced vendors for as-needed troubleshooting and resolution in support of the network.
- The customer may be notified depending upon the severity and type of problem.
- Trouble tickets are retained permanently so that NAEC 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:

NAEC'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. The AUP is posted on our website.

No Waiver/Severability:

Any failure of NAEC 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.

NAEC 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.

Version 1 Effective: 09/01/2024