Greeneville Energy Authority
Network Management Policy

Subject: Network Management Policy

Policy #: BB-100

Board Adoption: 11-7-2024

Effective Date: 11-7-2024

Approved By: GEA Board of Directors

Network Management Policy

Greeneville Energy Authority ("GEA") is committed to providing our customers with the best online experience possible. GEA 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 GEA not apply reasonable network management practices, our customers could be subject to the negative effects of, among other risks, security attacks, resulting in possible degradation of services. You may also access our most current Acceptable Use Policy (AUP) at

https://www.mygea.net/wp-content/uploads/Acceptable_Use_Policy_03102020-1.pdf.

Network Overview

GEA operates a state-of-the-art broadband network whereby fiber optic cable is brought past each home and business. GEA builds a fiber drop from the street to 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 GEA '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. GEA makes all efforts to ensure adequate bandwidth is available to all customers and reserves the right to employ congestion management practices in the future.

Application-Specific Behavior

Does GEA block or rate-control specific protocols?

1. GEA uses advanced monitoring technologies to identify various types of DDoS attacks. Once an attack has been identified certain traffic may be mitigated to protect GEA customers and network assets.
2. If GEA did not block and/or control these types of activities, GEA high speed internet customers could experience network instability and/or bandwidth slowdowns.
3. GEA does not block any other kinds of traffic. GEA subscribes to the philosophy of complete network neutrality, and we treat traffic to and from all customers the same.

Does GEA modify protocol fields in ways not prescribed by protocol standard? GEA does not modify protocol fields not prescribed by protocol standards.

Does GEA inhibit or favor certain applications or classes of applications? GEA does not inhibit or favor applications or classes of applications 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 GEA restrict the types of devices that it allows to to the network? GEA does not allow residential customers to switches or hubs directly to the IP port. A residential customer is limited to one (1) MAC address per service port. GEA also highly recommends business customers use a router and not a switch when connecting to our service.

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 the GEA Technical Support department at (423) 636-6200. 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?

GEA uses the following practices to ensure end-users security and network security:

1. GEA employs DHCP Option 82 –This is a protocol that attaches an identifier for all traffic on the network that tells the network what part of the network the traffic originated on.
2. GEA utilizes anti-spoof software which is intended to identify and isolate one user's hardware from impersonating another user's hardware.
3. The GEA network utilizes network separation, and the data from every customer is isolated from other users to stop unlawful access to specific traffic.

GEA utilizes these protocols and practices to protect and secure GEA customer data as well as to protect the GEA network for the benefit of all customers. These protocols allow GEA to comply with federal CALEA and other Law Enforcement requirements.

What conditions trigger a security mechanism to be invoked?

1. The DDOS protocols and practices used on the GEA fiber network provide far more protection from external malicious attacks than is available with other technologies.
2. As the Internet evolves, so do network attacks and other types of security exploits. GEA 's security tools and techniques are evolving to meet the security challenges of a 21st century world.
3. GEA monitors the network many times per second, and a trigger would be finding any instance of unwanted Denial of Service on the network. GEA 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 service offered, including Service Technology, Expected and Actual Speeds, Expected and Actual Latency, Suitability of the Service for Real-time Applications follows:

1. ***Service Technology***
    1. GEA uses an FTTH access system to deliver broadband services to customers. The FTTH system standard is based on XGSPON technologies. Up to sixty-four (64) customers share feed fibers in each neighborhood; this shared fiber is called a Passive Optical Network (PON). XGSPON delivers 10,000 Megabits per second to and from the subscribers on a PON.
    2. In the GEA 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 for our customers.
2. ***Expected and Actual Speeds***
    1. GEA offers High Speed Internet access speeds between 100 to 10,000Mbps in both directions. The expected speeds are the line rate of the subscribed package minus any network protocol overhead such as TCP and PON. Thus, 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 GEA network.
3. ***Expected and Actual Latency***
    1. 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 GEA network is designed to have a local operating latency as great as 5 milliseconds. However, in real practice, the actual local latency is generally around 4 milliseconds or less. The network distance and bandwidth constraints of the far end service being accessed will determine overall latency. GEA has no ability to control latency beyond its network edge.

4. ***Suitability of the Service for Real-time Applications***

    1. The GEA 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 GEA, 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 GEA 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 GEA may immediately suspend or terminate such User's service without issuing such a warning if GEA, 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. GEA 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 GEA exercise of its rights under this Policy. Additional requirements and/or penalties apply as found in GEA's Acceptable Use Policy (AUP).

Service Monitoring

GEA has no obligation to monitor individual 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 GEA with address, telephone number, email address, domain name, or URL, or any other personally identifiable information, permits GEA 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 GEA then applicable Privacy Policy and the requirements of applicable law.

Network Inspection

Do network management practices entail inspection of network traffic? GEA examines traffic to the extent needed to utilize the network safety features for intercepting network attacks. GEA does not inspect traffic for any purposes other than to keep track at the network level, where traffic flows 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, a lawful subpoena, or a valid public records request that requires disclosure.

Complaint Redress Options

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

1. GEA 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. Trouble tickets can be generated by customers or self-generated by alarms located on the GEA network.

2. Secondly, GEA 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 network glitch affecting one customer.

3. GEA attempts to identify and address problems from its Network Support Center (NSC). If the NSC is unable to clear a reported problem, then a technician in a truck is dispatched to address the problem.

4. If the problem is of such severity or of a nature 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. GEA contracts with experienced vendors for as-needed troubleshooting and resolution in support of the network.

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

6. Trouble tickets are retained permanently so that GEA can view a history of trouble at a specific customer site, a specific neighborhood or with a specific brand or piece of equipment.

Treatment of Inappropriate Content and Transmission

GEA reserves the right to refuse to transmit or post, and remove or block, any information, or materials, in whole or in part, that GEA, in its sole discretion, deems to be in violation of our posted Policies. While GEA has no obligation to monitor transmissions or postings made on the service GEA has the right to monitor these transmissions and postings for violations of GEA 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 child exploitation incident involving the internet contact law enforcement immediately. To report other violations of GEA policies, including the AUP, please contact GEA

Contact	Policy Agent
Mail	Greeneville Energy Authority Attn: Policy Agent P.O. Box 1690 Greeneville, TN 37744
E-mail	policy@mygea.net

No Waiver/Severability

Any failure of GEA 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.

GEA 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 November 7th, 2024