SandyNet Network Management Policy

Introduction

SandyNet and the City of Sandy are committed to helping provide our subscribers with the best online experience possible. The City of Sandy uses reasonable and acceptable network management practices that are consistent across the industry the help provide minimum disruptions to service connections. As networks change over time, our policies must also be adjusted. A lack of proactive network management practices may result in downtime, loss of service, susceptibility to cyber or security attacks and spam. The SandyNet Acceptable Use policy can be found on the SandyNet website.

Network Overview

SandyNet operates a fiber-to-the-x (FTTx) network, where fiber optic cables pass by every home and business within Sandy's civil limits. SandyNet constructs a fiber optic drop from its right-of-way (ROW) infrastructure to the premise to deliver broadband services. Prior to construction, access must be granted to SandyNet to construct and offer service by the property owner. Service cannot be constructed or offered without being granted a right to access.

Information Regarding SandyNet Network Practices

The Federal Communications Commission (FCC) requires SandyNet to provide descriptions of our Network Management Practices, including Application-Specific Behavior practices, Device Attachment Rules, Security Practices, Performance Characteristics, Privacy Policies and Subscriber Redress Options.

Congestion Management. Given SandyNet's current bandwidth capacity, no congestion management practice is currently required, and no active practice is being actively implemented within SandyNet's network. SandyNet reserves the right to employ appropriate and necessary congestion management practices in the future.

Application-Specific Behavior. SandyNet does not block outbound traffic protocols. SandyNet does filter inbound and outbound traffic that is identified as being malicious or invalid. SandyNet adheres to industry best practices for filtering inbound traffic, for the safety, protection, and experience of the subscriber. SandyNet does not block traffic, and supports and enforces the philosophy of network neutrality, and treats all traffic inbound and outbound traffic to be the same. SandyNet does follow standardized class-of-service (COS) models, for effective delivery of specific services. COS models include assigning priority towards latency specific applications, such as voice or television service, which prevents disruptions in service during micro bursting or any unforeseen network congestion.

Device Attachment Rules. By default, SandyNet limits subscribers to a single dynamic Internet Protocol (IP) address, for each service connection. That limit is raised through separate service charges or connections. Router or edge device specifics are covered under the security section of

this policy. SandyNet allows subscribers to utilize their own router, so long as the device meets the appropriate technology and has passed UL certification and carries FCC Part 64 certification.

Security. SandyNet employs industry standard security practices to ensure that subscribers and their services are protected from threats and attacks. SandyNet incorporates industry best practices for its usage of encryption protocols.

As the new vulnerabilities and security exploits are discovered, SandyNet implements security tools and procedures to mitigate or prevent those exploits. The usage of those tools and procedures help to protect service connections, subscribers, homes, and businesses that utilize our broadband services. These tools and techniques are compliant with law enforcement requirements.

SandyNet Actively samples and monitors the network for exploits, security vulnerabilities and other anomalies that can impact service. SandyNet works closely with law enforcement agencies as needed, and in the event of a breach or exploit.

Performance Characteristics. The following items are general descriptions of services offered by SandyNet, including the service technology, expected speeds and latency, and suitability of services.

Service Technology. SandyNet's FTTX network is used to deliver broadband services to homes, businesses, smart city initiatives and other governments or agencies. The FTTX network is largely built using a Passive Optical Network (PON) technology, which utilizes a technology called Time Division Multiplexing (TDM) to allocate talk and listen times, allowing up to 32 subscribers for each backbone fiber line.

Expected and Actual Speeds. Depending on the actively deployed generation of PON technology, max speeds offered per strand of fiber can reach 10 Gigabits per second (Gbps) for both up and down speeds. Speeds lower than the maximum ceiling value are due to a subscribers selected service packages, the nature of the public internet, as well as in home technology and interference, such as noise or overlapping WiFi frequencies. Individual devices may train up at a speed higher than the device's capability throughput, and network packet overhead can decrease the end-to-end throughput. Because this decrease in speed is observable, SandyNet attempts to offset the network overhead by increasing the actual speed when possible. Due to the max train rate of a device or connection, this offset is not always possible, and therefore actual and expected speeds may vary upwards of 15% of the advertised speed. For half gigabit subscribers, speeds are offset, so subscribers regularly get higher than 500 Megabits per second (Mbps) speeds. Gigabit subscribers typically see 960Mbps with overhead and a 1Gbps train rate for their devices. 2Gbps subscribers with a 2.5Gpbs or 10Gbps train rate can seed the full 2Gbps up and down. Subscribers with the 5Gbps service should see the same 5Gbps speeds for both up and down connections.

Expected and Actual Latency. Latency is used to measure the time it takes to transmit and receive information from network source and its destination. Latency is often measured in milliseconds, and latency can fluctuate. That fluctuation is measured as the delta between the

upper and lower latency observed during a time. That delta is known as jitter, which represents the stability of the connection. SandyNet does not set a maximum level of latency, due to the nature of the public internet, the source and destination of the connection or unforeseen or unmitigated network congestion. SandyNet considers latency inside of its network (any device managed by SandyNet) to not exceed 20ms latency. Actual latency is typically less than 3ms for internal connections. Legacy systems or other wireless point-to-point or point-to-multipoint may experience higher jitter due to the nature of the connection or medium, interference, or state of the hardware.

Suitability for Real-time Applications. SandyNet offers some of the fastest networks in the U.S. Subscribers can access information and content 24/7, without slowdowns or network blockages or congestion.

System and Network Security

Users are prohibited from violating or attempting to violate the security of SandyNet, 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 measure 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, forging any packet header or any part of the header information in any E-mail or newsgroup posting, 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 and Termination

Any User which SandyNet 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 SandyNet may immediately suspend or terminate such user's service without issuing such a warning if SandyNet, in its sole discretion deems such action necessary. If we determine that a User has committed as 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 eliminated or preclude such violation. SadnyNet shall not be liable for any damages of any nature suffered by any subscriber, User, or any third party resulting in whole or in part from SandyNet exercise of its rights under this Policy. Additional requirements and/or penalties apply as found in SandyNet's Acceptable user Policy (AUP).

Service Monitoring

SandyNet has no obligation to monitor the services but may do so and disclose information regarding the use of the service for any reason if we, in our sole discretion, believe that it is reasonable to do so, including to satisfy laws, regulation, 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 or providing SandyNet with and address, telephone number, E-mail address, domain name, URL, or any other personally identifiable information, permits SandyNet to use such information for commercial purpose 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 SandyNet then-applicable Privacy Policy and the requirements of applicable law.

Impact of Specialized Services

SandyNet offers services that could be considered a "Specialized" service over its access system. This includes voice services, video services or other agreed upon managed services.

Voice services are largely separated from the broadband access services discussed in this policy and will not affect a subscriber's access to the open internet. Proper COS levels prevent voice services from affecting broadband services.

Television is a similar setup, with a higher bandwidth constraint, where each concurrent video stream may result in up to 20Mbps of traffic, and in high usage cases, may result in prioritization over general broadband access. There are no use cases where television service will disrupt a subscriber's access to the internet.

Network Inspection

SandyNet does not inspect traffic for any other purposes than to internally monitor or track network level statistics. These statistics are used to identify trends, threats and monitor the network health and network operational capacity.

SandyNet does collect flow information, which is used both internally and sent to a third-party for aggregation and association to subscriber accounts. Flow data provides helpful statistics for SandyNet, which can help troubleshoot or diagnose subscriber issues. Additionally, flow data is abstracted to a high level to identify markets and other information that may be useful for SandyNet's internal marking team. By design, flow data is ambiguous, and aggregates based on IP address blocks, ports, autonomous system numbers, and protocols.

SandyNet may share inspected network traffic with valid and qualified law enforcement agencies, upon a court order.

Complaint Redress Options

SandyNet will log all complaints as a trouble ticket in our helpdesk system. This helps identify trends or other issues that similar subscribers may have. Tickets can be generated by agents, the individual subscriber or automatically through network monitoring systems.

SandyNet prioritizes each trouble ticket base upon the perceived severity of the problem. This severity may be influenced by metrics, number of similar reports, service level agreements, etc.

SandyNet will attempt to identify and correct the problem over the phone or E-mail. If necessary, the issue may be escalated to the Network Operations Center (NOC) team for analysis and root cause analysis. If NOC cannot resolve the issue, a service technician may be dispatched to the affected area or address to resolve the issue.

If the problem cannot be resolved by an on-site technician, a Network Engineer or Manager may get involved to help resolve the situation. If an outside consultant or vendor is required to resolve the issue, the General Manager will be involved to help facilitate each party until the issue is resolved.

The Subscriber shall be notified periodically or as needed throughout the resolution process.

Treatment of Personal Servers

Subscribers and Users are solely responsible for all information published or stored on any Personal Web Server and/or File Servers and for ensuring that all content and information is appropriate for those who may have access to it. This includes taking 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 files/recordings, images, and illustrations. SandyNet reserves the right to remove or block content contained on personally hosted web sites or file systems if SandyNet, in its sole discretion, determines that it violates the terms of the SandyNet Acceptable Use Policy.

Treatment of Inappropriate Content and Transmission

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

No Waiver/Severability

Any failure of SandyNet 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.

SandyNet 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.