Network Management Practices Disclosure

Consistent with FCC regulations[1], U.S. TelePacific Communications, Corp. d/b/a TPx Communications and its subsidiary(s), referred to as "TPx", provides this information about our Broadband Internet Access Service and may be subject to updates and revisions. Customers are encouraged to review them on a regular basis.

- **Blocking.** TPx does not engage in any practice, other than reasonable network management disclosed herein, that blocks or otherwise prevents end user access to lawful content, applications, service, or non-harmful devices.
- **Throttling.** TPx does not engage in any practice, other than reasonable network management disclosed herein, that degrades or impairs access to lawful Internet traffic on the basis of content, application, service, user, or use of a non-harmful device.
- **Affiliated or Paid Prioritization**. TPx does not engage in any practice that directly or indirectly favors some Internet traffic over other traffic to benefit an affiliate or in exchange for consideration, monetary or otherwise.

Congestion management. This section describes our network management practices used to address congestion on our network.

- **Network monitoring.** We monitor our network at an aggregate level for utilization trends. We receive regular reports showing changes in network traffic and congestion. We use this information to plan increases in available bandwidth, port additions or additional connectivity to the Internet. Should new technologies or unforeseen developments in the future make it necessary to implement an active congestion management program, we will update these disclosures and otherwise notify our customers of the scope and specifics of this program.
- **Potential heavy bandwidth users.** We monitor end user usage for identification and management of potential heavy bandwidth users in relation to 4G. TPx may contact these customers whose bandwidth usage is considered excessive to try to help those customers find an Internet plan that better suits their needs.
- **Types of traffic affected.** Our congestion management practices do not target any specific content, applications, services, or devices, or otherwise inhibit or favor certain applications or classes of applications.

[1] 47 C.F.R. § 8.1; Preserving the Open Internet, Broadband Industry Practices, Report and Order, 22 FCC Rcd 17905 (2010); Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015); Restoring Internet Freedom, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2017).

Application-Specific Practices. This section discloses any application-specific practices we use, if any.

- **Management of specific protocols or protocol ports.** To protect the security of our network and our customers, we may block known hostile ports. In such cases, we may block that specific port to enforce our Acceptable Use Policy ("AUP") until the attack ceases, at which time we remove the block. The AUP is available at https://www.tpx.com/legal/acceptable-use-policy/.
- **Modification of protocol fields.** Not applicable.
- **Applications or classes of applications inhibited or favored.** Not applicable.

Device Attachment Rules. This section addresses any limitations on attaching lawful devices to our network.

- **General restrictions on types of devices to connect to network.** We place no general restrictions on lawful devices that a customer may connect to our network, so long as the device is: (i) compatible with our network; and (ii) does not harm our network or other users. Our broadband Internet service works with most PCs and laptops including Macs, and other Internet compatible devices like game systems and Internet-enabled TVs. If a password-protected wireless router is connected to our broadband Internet service, wireless Internet compatible devices properly connected to the router including computers, tablets, smartphones, and other devices can connect to our network. If a customer or potential customer believes they have an unusual configuration, our customer service department will help determine if there is a compatibility problem.

Network and End User Security. This section provides a general description of the practices we use to maintain security of our network.

- TPx assumes no liability and makes no guarantee, either expressed or implied, for the security of any data on any of its servers, whether or not they are designated as "secure servers.
- TPx customers are responsible for maintaining security of their networks to prevent their use by others in a manner that violates this AUP. The TPx Network may not be used in connection with attempts—whether successful or not—to violate the security of a network, service, or other system (hacking).
- **Unintentional Harm:** With or without proper security measures in place, any network connected to the Internet can receive traffic coming from other locations on the Internet. The open nature of Internet communications is subject to abuse and users should implement measures to prevent unwanted and malicious traffic to their network. This can be accomplished through the use of a properly configured firewall and using best practice security measures. TPx assumes no liability for any harm to a customer resulting from the use of TPx's Service.
- **Denial of Service (DOS) Attacks:** TPx reserves the right to take any action necessary to protect its network and service from denial of service attacks or any other malicious activities that may be directed at the customer through no fault of their own. Such actions may include but are not limited to null routing a customer IP for an indefinite period of time without warning.
- **Impending Security Event Notification:** TPx users are responsible for notifying TPx immediately if they become aware of an impending or occurring event that may negatively affect the TPx network. This includes but is not limited to extortion threats that involve threat of "denial of service" attacks, unauthorized access, or other security events.

Incident Reporting, Response and Remediation. This section provides a general description of TPx's handling of incidents.

- TPx occasionally is required to investigate potential abuses brought to our attention by on-going monitoring, other ISPs, or other users of the Internet. If you have any complaints about activity that may be in violation of this Acceptable Use Policy (AUP), you may submit them to abuse@tpx.com. These notifications may or may not reflect an actual violation of this AUP. To this end, TPx will investigate the nature of the abuse reported, and reserves the right to contact any TPx customer in the process of completing this investigation. Customers must update their authorized contact list with TPx so that the customer can be informed of any disruption of service or abuse occurring on their network. Customers are obligated to respond within twenty-four (24) hours to any such requests for information to allow closure of such items. In the event that a violation of any of these policies is identified, TPx customers are obligated to cease the offending activity or activities immediately. Failure to do so may result in limitations being placed on the quantity or type of traffic TPx will forward to the Internet for the affected customer, termination of service, or other remedies deemed reasonable by TPx until the customer has demonstrated to TPx's satisfaction that such behavior will not be repeated.

- TPx reserves the right to take immediate action upon receipt of notification or discovery of any violation of the Acceptable Use Policy without notice to the customer. In the event that such action is taken, TPx will contact an authorized contact of the affected company.

- At times, network and computing system problems may occur. During these unlikely events, it may be necessary for TPx to examine system accounting logs and other records. Therefore, TPx reserves the right to access a customer's email accounts and file space hosted on TPx servers as needed to resolve system problems and to monitor accounts for system utilization, system optimization, and billing purposes. TPx also reserves the right at any time to monitor customer bandwidth, usage, transmissions, content and conduct security scans to identify violations of the AUP and/or to protect the network, the service and TPx users.

- **Suspension or Removal of Violators**: In some cases, TPx may determine that a customer must be permanently removed from the TPx network. Permanent removal of the subscriber's account from the TPx system does not relieve the violating customer of any responsibility for payment under the terms of the Service Agreement, which may include liability for the balance of the remaining term of service. TPx reserves the right to immediately terminate subscriber's service if, in TPx's sole discretion, subscriber has abused access facilities.

General Service Description. TPx is a Managed Services Provider, delivering unified communications, managed IT and network connectivity to customer locations across the country. TPx offers Managed MPLS, VPLS, EPL network services, SD WAN connectivity, SIP Trunking, PRIs, business lines and last mile access – Ethernet over Copper, Fixed Wireless and NNI Capabilities. Additional Service information is available at https://www.tpx.com/services/communications-collaboration/.

Expected and actual speeds and latency.

- **Expected performance.** We offer customers a variety of broadband Internet service levels. Our Packet-Based Services Service Level Agreement and TDM Services Service Level Agreement is available at https://www.tpx.com/legal/sla/.
- **Speed.** The speeds we identify for each broadband Internet service level are the maximum upload and download speeds that customers are likely to experience. We provision our customers' modems and engineer our network to deliver the speeds to which our customers subscribe. However, we do not guarantee that a customer will actually achieve those speeds at all times. A variety of factors can affect upload and download speeds, including customer equipment, network equipment, transport and networking protocols, congestion in our network, congestion beyond our network, performance issues with an Internet application, content, or service, and more.
- **Latency.** Latency is another measurement of Internet performance. Latency is a term that refers to the time it takes for information to travel between your computer and your Internet destination. High latency occurs when the time it should normally take for the information to make the trip becomes abnormally long. Latency is typically measured in milliseconds, and generally has no significant impact on typical everyday Internet usage. Most applications, such as email and websites, work well despite average latency. Highly interactive applications, such as multi-player games, do not work well with higher latency. As latency varies based on any number of factors, most importantly the distance between a customer's computer and the ultimate Internet destination (as well as the number and variety of networks your packets cross), it is not possible to provide customers with a single figure that will define latency as part of a user experience. Additional information is available at https://www.tpx.com/legal/sla/.
- **Actual speed and latency performance.** The actual speed and latency experienced by individual users may vary depending upon network conditions and other factors. Actual performance of our Cable Modem service in most cases will conform to national wireline broadband Internet speed and latency levels reported by the FCC.
- **Customer Speed Test.** We provide an online speed test for our customers, available at https://www.tpx.com/resources/bandwidth-speed-test/.

Suitability of the Service for Real-time Applications. Our broadband Internet access service is suitable for typical real-time applications, including messaging, voice applications, video chat applications, gaming, and Internet video. If users or developers have questions about particular real-time applications, please contact us 877-487-8722 or https://www.tpx.com/contact-support/contact-us/.

Non-Broadband Internet Access (BIAS) Data Services.

- **Non-BIAS Data services offered to end users.** We offer several managed or "non-BIAS data" services over our network, sharing network capacity with other high speed Internet services. Managed non-BIAS data services include Voice over Internet Protocol (VoIP), Internet Protocol video, and dedicated bandwidth to high volume business users.
- **Effects of non-BIAS data services on availability and performance of broadband Internet access service.** Our provision of non-BIAS data services has no effect on the availability and performance of our broadband Internet access service.

COMMERCIAL TERMS

- **Prices.** Fees will be billed as specified in your contracted agreement, rate plan brochure, customer service summary, or rate plan information online.
- **Fees for early termination.** An early termination fee may be charged if a customer disconnects while under a contracted agreement. Additional information is available at https://www.tpx.com/legal/terms-conditions/.

Additional pricing information is available on our website at https://www.tpx.com/legal/rates-fees.

Privacy Policies. U.S. TelePacific Corp., dba TPx Communications, is committed to protecting your privacy. This statement applies to data collection and usage policies on all TPx-owned sites and services, unless otherwise noted. TPx logs the pages our visitors go to, including time spent within our web sites, in order to gauge popularity and determine what sites and services need improvement. In addition to information that is submitted from our visitors when contacting TPx or placing an order, we also collect certain information about your computer and network systems. Information collected includes, but is not limited to: visitor IP address, operating system software, browser software and version, visit date and times, referring web site URLs, and search engine terms used to find our site. TPx collects your personal information in order to operate and deliver services requested by our customers. We also use your personal information to inform you of the availability of other related services and other information. TPx does not sell your personal information. However, we may contact you on behalf of our business collaborators about particular offerings that may be of interest to you. TPx also may share your personal information with contractors we have hired (or will hire) to provide services to us or on our behalf. These contractors are (or will be) contractually bound to use such personal information we share with them only to perform the services for which we contracted (or will contract) with them. TPx may disclose your personal information: (i) if you direct us to do so, (ii) if required by law, and/or (iii) in some other circumstances, including, but not limited to, for the purpose of protecting from fraud, protecting the rights and/or property of TPx, or protecting the rights, property, and/or information of our customers). TPx uses 128-bit SSL (Secure Sockets Layer) encryption technology, the industry standard, when transmitting all data to and from your computer and our servers, including your name, address, phone, email, and credit card information. The servers on which your data is stored have limited access and are located in controlled server environments. We protect your personal information when orders are submitted through our web site, and when performing any function within our Account Management area. TPx uses cookies to help improve our website and web hosting services, and to improve our visitors' overall user experience. Third party vendors, including Google, show TPx ads on sites on the internet. Third party vendors, including Google, use cookies to serve ads based on a user's prior visits to TPx's website. Users may opt out of Google's use of cookies by visiting the Google advertising opt-out page and/or the Network Advertising Initiative opt out page.

Links to External Web Sites. This site may contain links to other sites. While we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content, security, or privacy policies employed by other sites. Please review their respective policies before submitting your personal information.

Provision of aggregate or anonymized network traffic information to third parties. We may disclose aggregate or anonymized network traffic information to third parties for purposes of providing and managing our broadband Internet service or if required by law.

Use of network traffic information for non-network management purposes. We do not use network traffic information for non-network management purposes. However, data regarding a customer's excessive data usage may be utilized for discussions to move that customer to a higher broadband plan.

Redress options. We welcome questions about our broadband Internet access service. This section discloses redress options.

- **End user complaints and questions.** End users with complaints or questions relating to these disclosures should contact 877-487-8722.
    - **Questions.** We will endeavor to answer questions promptly via email or voice.
    - **Complaints**. For written complaints, a customer service representative will contact the end user via phone call. We will attempt to resolve complaints informally, escalating the matter to senior management if needed.

To submit complaints to the FCC, you can contact the FCC by phone at 1-888-225-5322, or online at https://consumercomplaints.fcc.gov/hc/en-us.