INTERNET TRANSPARENCY POLICY

In accordance with FCC regulations (47 CFR § 8.1(a)) applicable to all providers of broadband Internet access service, the City of Loveland's Electric and Communications Enterprise ("Pulse") provides the following information concerning its network management practices, the service's performance characteristics, and commercial terms. If you have any questions about the following network practices, please contact us at PulseInfo@LovelandPulse.com *or (970)-962-2010.*

NETWORK MANAGEMENT PRACTICES

Blocking. Pulse does not undertake any practice, other than reasonable network management elsewhere disclosed, that blocks or otherwise prevents end user access to lawful content, applications, service, or non-harmful devices.

Throttling. Pulse does not degrade or impair access to lawful Internet traffic on the basis of content, application, service, user, or use of a non-harmful device.

Affiliated Prioritization. Pulse does not directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, or resource reservation, to benefit an affiliate, including identification of the affiliate.

Paid Prioritization. Pulse does not directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, or resource reservation, in exchange for consideration, monetary or otherwise.

Congestion Management. Pulse uses reasonable network management practices that are consistent with industry standards. Pulse uses various tools and techniques to manage its network and deliver its services. These tools and techniques are dynamic and can and do change frequently. Network management activities may include identifying spam and preventing its delivery to customer email accounts, and detecting malicious Internet traffic and preventing the distribution of, or inadvertent access to, malware, phishing, viruses, or other harmful code or content.

Pulse currently does not maintain a separate system to assist with managing times of congestion. As Pulse's network technologies and usage of the network continue to evolve, Pulse reserves the right to implement a new congestion management system if necessary in the performance of reasonable network management and in order to maintain a good broadband Internet access service experience for our customers, and will provide updates here as well as other locations if a new system is implemented.

Application-Specific Behavior*.* Pulse does not block or rate-control specific protocols or protocol ports, or otherwise inhibit or favor certain classes or applications.

Device Attachment Rules. Pulse does not impose any restrictions on the types of devices or any approval procedures for devices to connect to the Pulse network, provided they are used for lawful purposes and do not harm the Pulse network or other services, violate Pulse's Terms and Conditions, or harm other users of the Pulse network. However, if Pulse determine, in its sole discretion, that the connection of a particular type of device negatively affects the network, impacts other users, or may expose Pulse to potential legal liability, Pulse reserves the right to limit or restrict a user's ability to connect such device.

Security. Pulse employs a number of practices to help prevent unwanted communications, such as spam, and protect the security of Pulse's customers and network. Pulse limits the number of login, simple network management protocol (SMTP), domain name system (DNS), and dynamic host configuration protocol (DHCP) transactions per second (at levels far above "normal" rates) that customers can send to Pulse servers in order to protect them from denial of service attacks. Pulse does not disclose exact rate limits in order to maintain the effectiveness of these measures.

In order to further protect our customers, Pulse blocks a limited number of ports that are commonly used to send spam, launch malicious attacks, or steal a customer's information. Pulse conducts security initiatives, and offers security tools for our customers.

Pulse's subscriber management is enforced by a set of authentication steps, security and quality of service features allowing automatic subscriber provisioning and per customer quality of service and security enforcement. If authentication fails, subscriber traffic will be dropped due to anti-spoofing security protocols. All events are logged for analysis and protocol authentication is used to prevent intruders from physically connecting unauthorized equipment to Pulse's network.

PERFORMANCE CHARACTERISTICS

Service Description. A current description of the categories of internet access services offered to residential and commercial users, including actual access speed and latency can be found online at www.LovelandPulse.com/service-description-and-performance-characteristics/.

Impact of Non-Broadband Internet Access Service Data Services. Pulse does not offer data-related specialized services to users that will affect the capacity available for, and performance of, Pulse's broadband internet access service data service.

COMMERCIAL TERMS AND PRIVACY

Price. A schedule of current pricing for Pulse services can be found online at www.LovelandPulse.com/RateCard.

Privacy Policies. Pulse is committed to protecting the privacy of its customers. Pulse's current Privacy Policy can be found online at www.LovelandPulse.com/Privacy.

QUESTIONS

If you have any questions about these disclosures, cannot find what you are looking for, or have any other concerns about Pulse Internet services, please contact the Pulse Municipal Fiber Manager at PulseLegal@cityofloveland.org. Pulse will review and promptly respond to all submissions.