CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY

The City of Loveland's Electric and Communications Enterprise ("Pulse") has adopted and implemented procedures and policies to ensure compliance with the Federal Communications Commission's ("FCC") Customer Proprietary Network Information ("CPNI") Rules. Pulse's CPNI procedures are as follows:

CPNI USE

Pulse shall not use, disclose or permit access to CPNI without approval of the customer except to:

a) Initiate, render, bill, and collect for services;
b) To protect the rights and property of Pulse and other telecommunication service providers from fraudulent, abusive or unlawful use of, or subscription to services;
c) To provide inside wiring installation, maintenance, and repair services; or
d) As required by law.

Without customer approval, Pulse shall not use, disclose or permit access to CPNI to provide or market service offerings within a category of service to which the customer does not already subscribe.

Pulse does not currently engage in, disclose, or permit access, to CPNI to provide or market service offerings within a category of service to which the customer does not already subscribe.

CPNI APPROVALS

When customer approval to use, disclose, or permit access to customer CPNI is required, Pulse shall obtain approval through written, oral or electronic methods. If Pulse relies on oral approval, Pulse understands that such approval must be given in compliance with the FCC's CPNI rules. Pulse shall honor a customer's approval or disapproval until the customer revokes or limits such approval or disapproval. Pulse shall maintain records of all customer approvals for at least one year. Sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

If Pulse discloses or allows access to a customer's individually identifiable CPNI to Pulse's independent contractors, Pulse will require, in order to safeguard that information, the contractors' entry into confidentiality agreements that:

a. Restrict them to using the CPNI solely for providing the communications-related services for which they are engaged and for which the CPNI has been provided;
b. Prohibit their subsequent permitting of any third-party to use, allow access to, or disclose the CPNI, unless the third-party is required to make disclosure under force of law; and
c. Require that they have in place appropriate protections to ensure the ongoing confidentiality of the CPNI.

CPNI NOTICE REQUIREMENTS

Pulse shall notify each customer of his or her right to restrict the use or disclosure of, and access to, CPNI along with a solicitation of approval, in compliance with FCC rule section 64.2008. Pulse's notifications shall:

a. Contain a statement that the customer has a right, and Pulse has a duty, under federal law, to protect the confidentiality of CPNI; and
b. Specify the types of information that constitute CPNI and the specific entities that will receive CPNI, describe the purposes for which the CPNI will be used, and inform the customer of his or her right to disapprove those uses and deny or withdraw access to CPNI use at any time.

Pulse shall advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and Pulse shall clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes.

In addition, for "opt-out" approvals, Pulse shall wait at least thirty (30) days after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI and notify customers of the applicable waiting period for a response before approval is assumed.

CPNI SAFEGUARDS

Pulse has implemented procedures for customer privacy in accordance with 47 C.F.R. section 222, and the FCC's implementing regulations. As part of its privacy procedures, Pulse has trained its personnel as to when they are, and are not, authorized to use CPNI, and has adopted a supervisory review process to ensure compliance with CPNI rules, as well as an express disciplinary process to deal with employee failures.

Pulse authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-office visit. Pulse shall disclose CPNI to a customer in person at our office location(s) only when the customer presents a valid photo ID and such ID matches the name on the account. Pulse shall disclose call detail information in a customer-initiated call only in the following cases:

a. After the customer provides a pre-established CPNI security password; or
b. At the customer's request, by sending the information to the customer's address of record, or by calling back the customer at his or her telephone number of record.

Pulse has established security passwords with customers in order to authenticate customers. Neither security passwords nor the backup method for authentication rely on customers' readily available biographical information. Pulse has established password protection for customers' online accounts. Pulse shall notify a customer immediately of changes with a customer's password, a customer's security PIN, a customer's response to back-up means of authentication, online account, or address of record.

CPNI RECORDKEEPING AND REPORTING

Pulse does not currently use its customers' CPNI for marketing campaigns.

Pulse has designated a corporate officer who will sign a compliance certificate on an annual basis stating that such corporate officer has personal knowledge that Pulse has established operating procedures adequate to ensure compliance with all applicable CPNI rules. Pulse shall provide a statement accompanying the certificate that explains Pulse's operating procedures and demonstrates compliance with the CPNI rules.

Pulse is prepared to provide written notice within five (5) business days to the FCC of any instance where the opt-out mechanisms do not work properly to such a degree that consumers' inability to opt-out is more than an anomaly. That notice would be in the form of a letter and would, at a minimum, include:

a. Pulse's name;
b. A description of the opt-out mechanism(s) used;
c. The problem(s) experienced;
d. The remedy proposed and when it would be/was implemented;
e. Whether Pulse has notified relevant state commissions/authorities and what action, if any, was taken;
f. A copy of any notice provided to customers; and
g. Contact information.

Pulse shall submit the notice even if other methods by which consumers may opt-out are offered.

Pulse is prepared to notify the U.S. Secret Service and FBI within seven (7) business days after its discovery of any intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of, CPNI. Pulse will also notify the customer of such breach, after consulting with the investigatory agency(ies), if Pulse believes there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. Pulse will notify the customer of the breach after seven (7) business days following notification to the FBI and Secret Service, if such agencies have not requested that Pulse postpone disclosure to the customer.

Pulse will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two (2) years.