

## OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

Spencer Municipal Utilities (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

### Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

### Employee Training:

The Compliance Officer arranges for the training of all employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. Training includes notice to employees that the CPNI manual is housed in the Compliance Officer's office.

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

### Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all employees.

The Company's disciplinary process is part of the employee personnel policy. Employees have access to this policy on the company network.

### Customer Notification and Request for Approval to Use CPNI

The Company has provided notification to its customers of their CPNI rights and has asked for the customer's approval to use CPNI via the opt-out method. A copy of the notification is also provided to all new customers that sign up for service.

The status of a customer's CPNI approval is prominently displayed as soon as the customer's account is accessed so that employees can readily identify customers that have restricted the use of their CPNI.

For the customers that have opted-out and said the Company cannot use their CPNI, that decision will remain valid until the customer changes it.

The company sends the opt-out notice every two years to those customers that have not previously opted out.

The Company will provide written notice within five 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.

A copy of the most recent notification is kept in the CPNI official files.

### Marketing Campaigns

If the Company uses CPNI for any marketing campaign, the Compliance Officer will review the campaign and all materials to ensure that it is in compliance with the CPNI rules.

The Company has a process for maintaining a record of any marketing campaign of its own, or its affiliates, which uses customers' CPNI.

### Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

**In-office visit** - the customer must provide a valid photo ID matching the customer's account information.

**Customer-initiated call** – the customer is authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

If the customer wants to discuss call detail information that requires a password, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.
- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

### Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Address of record.

The notification to the customer will be made either by a Company-originated voicemail or text message to the telephone number of record or sent to the postal address of record.

The Company has a process for tracking when a notification is required and for recording when and how the notification is made. The billing software generates a message stating that the customer must be notified. The CSR then either calls the customer or sends the software generated letter to the customer. Information about the notification is noted in the software.

### Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.
- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.
- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.
- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.
- Include a summary of the breach in the annual compliance certificate filed with the FCC.

### Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

### Record Retention

The Company retains all information regarding CPNI. Following is the minimum retention period we have established for specific items:

- CPNI notification and records of approval – one year. Stored in customer files.
- Marketing campaigns – one year. Stored in CPNI official files.
- Breaches – two years. Stored in CPNI official files.
- Annual certification – five years. Stored in CPNI official files.
- Employee training certification – two years. Stored in CPNI official files
- All other information – two years. Stored in CPNI official files