# Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

# EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: February 28, 2018

2. Name of company(s) covered by this certification: Great Plains Broadband, Inc.

3. Form 499 Filer ID: 826228

4. Name of signatory: Janelle Allison

5. Title of signatory: COO/CFO

6. Certification:

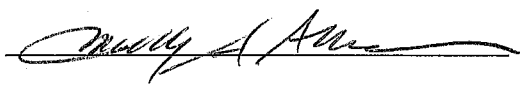
I, Janelle Allison, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq*. of the Commission's rules.

The company has not taken actions (*i.e.,* proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

**Attachments:** Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (if applicable)
Summary of customer complaints (if applicable)

# OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

Great Plains Communications, Inc. (Parent Company)
Great Plains Broadband, Inc.
Great Plains Communications Long Distance, Inc.

Great Plains Communications, Inc., Great Plains Broadband, Inc., and Great Plains Communications Long Distance, Inc., (the "Companies") have 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), section 64.2001 through section § 64.2011.

## Compliance Officer

The Companies have appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Companies are 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. The Companies have assigned as their Compliance Officer, Janelle Allison, COO, CFO.

## Employee Training

The Compliance Officer arranges for the training of all employees on an annual basis, and more frequently as needed. Any new employees are trained when hired by the Companies. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the Companies is using. The details 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 Companies procedures for protecting CPNI and they understand the Companies disciplinary process for improper use of CPNI. Each employee receives a copy of the Companies Operating Policy with their Employee Manual during orientation.

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 Companies have established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type of 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.

A copy of the Companies disciplinary process is included with the CPNI Operating Policy and is included with each Employee Manual and posted on the Employee website.

Customer Notification and Request for Approval to Use CPNI

The Companies have 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 Companies cannot use their CPNI, that decision will remain valid until the customer changes it.

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

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

Authentication

The Companies do 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 must provide his/her pre-established password and must be listed as a contact on the account. If the customer cannot provide the password or the answer to the back-up authentication, the customer is re-authenticated, without using readily available biographical information or account information, and a new password is established.

Notification of Account Changes

The Companies promptly notify customers whenever a change is made to any of the following:

- Password
- Address of record
- Contacts added to the account

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 address (postal or electronic) of record.

The Companies have a process for tracking when a notification is required and for recording when and how the notification is made. The current process is done manually. With future enhancements to our billing software, a program will automatically generate the letters to be sent out.

Notification of Breaches

Employees will immediately notify their Supervisor who in turn will 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 Companies retain all information regarding CPNI in a CPNI file. Following is the minimum retention period we have established for specific items:

- CPNI notification and records of approval – one year
- Marketing campaigns – one year
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years