BRANDENBURG TELEPHONE COMPANY

P.O. Box 599
200 Telco Drive
Brandenburg, KY 40108
270-422-2121

BEFORE
THE FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554
EB Docket No. 06-36

ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION

Annual 64.2009(e) CPNI Certification for 2018

Date filed: February 18, 2019

Name of company covered by this certification: Brandenburg Telephone Company, Inc.

Form 499 Filer ID: 801339 FRN: 0004995429

Name of signatory: Allison Willoughby

Title of signatory: General Manager

I, Allison Willoughby 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system or at the Commission) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

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

Signed: _____
Allison Willoughby
General Manager

Dated: February 18, 2019

BRANDENBURG TELEPHONE COMPANY

P.O. Box 599
200 Telco Drive
Brandenburg, KY 40108
270-422-2121

Brandenburg Telephone Company, Inc. – FCC 499 Filer ID: 801339 FRN: 0004995429

P.O. Box 599 Brandenburg, KY 40108

STATEMENT OF FCC CPNI RULE COMPLIANCE

This statement serves to explain how Brandenburg Telecom LLC (collectively the "Company") is complying with Federal Communications ("FCC") rules related to the privacy of customer information. The type of information for which customer privacy is protected by the FCC's rules is called "customer proprietary network information" ("CPNI"). The FCC's rules restricting telecommunications company use of CPNI are contained in Part 64, Subpart U of the FCC's rules (47 C.F.R. § 64.2000-2009).

1. Duty to Protect CPNI

We recognize our duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

i: Administrative use: We may use CPNI to initiate, render, bill and collect for communications services.

ii: Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.

iii. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

2. Our use of CPNI in Marketing

The Company does not use CPNI for marketing purposes except in the following circumstances:

i: to market services to our existing customers within the categories of service to which the customer already subscribes.

ii: to provide CPE and call answering, voice mail or messaging, voice storage and

retrieval services, fax store and forward, and protocol conversion.

For marketing purposes for which use of CPNI would otherwise require permission from the Customers, the Company uses only Customer billing name and address and/or telephone number without and segregation or refinement based on CPNI. On inbound and administrative calls, however, the Company may utilize CPNI in its sales and marketing efforts by first requesting permission to do so pursuant to §64.2008 (f). In those cases, the Company recognizes that permission to use CPNI ends when the call terminates and the Customer is fully informed that they may refuse the permission.

We regularly review our marketing practices to determine when, how and if CPNI is used within the Company to insure that we remain in compliance with the FCC's CPNI regulations and with our policy as described here in. In the unlikely event that Company decides to modify its policies for use of CPNI, it will insure that its new policy fully complies with FCC CPNI rules including, but not limited to, tracking and customer notice provision contained in §64.2008-2009.

1. Authentication Prior to Disclosure of CPNI

We understand that we are required to determine that any request for CPNI will not be released without authentication the authority of the requestor to receive such information.

We understand that when a customer calls, we may not release CPNI until we have authenticated the release of the information to the requestor in a manner consistent with CPNI regulations.

2. Employee Issues

All of our employees were trained regarding the company's CPNI policies which were effective December 8, 2007. To maintain compliance with FCC rules after December 8, 2007, the Company developed a manual and identified a compliance officer to address any CPNI-related issues that may arise. The Company has established procedures and trained employees having access to, or occasion to use customer data, to identify what customer information is CPNI consistent with the definition of CPNI under the FCC's revised CPNI rules.

The Company has implemented a training procedure for all new hires and contractors regarding the Company's practices regarding CPNI.

In addition, the Company has in place an express disciplinary process to address any unauthorized use of CPNI where the circumstances indicate authorization is required under the FCC's CPNI rules.

3. Notifications to Customers

We notify customers when changes have been made to passwords (if applicable), addresses of record, and authorized users by mailing a notification to the account address of record. The notice does not contain information regarding the changes.

4. Record-Keeping

We maintain the following records in our files for at least two years:

i. Employee disciplinary records, if applicable; and

ii. If applicable: 1) records of discovered CPNI breaches 2) notifications to law enforcement regarding breaches, and 3) any responses from law enforcement regarding those breaches.

5. Unauthorized Disclosure Of CPNI

We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at http://www.fcc.gov/eb/CPNI/ to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinary urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Signed _____

Allison Willoughby
President

Dated: February 18, 2019