CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY AND PROCEDURES

June 2024

Introduction

The protection of our customers' privacy is of utmost concern to Tularosa Communications ("TC" or "Company") and its employees. The proper handling of our customers' confidential information is not only the responsible and right thing to do - it is a requirement under federal law. This document describes TC's current policy and procedures regarding the Customer Proprietary Network Information (CPNI). It includes training material for employees and other information concerning the company's current and ongoing efforts regarding compliance with applicable Federal CPNI standards. Employees are required to read, understand and comply with all provisions described in the following pages.

The Company may have the need from time-to-time to modify its policy and procedures regarding CPNI in order to maintain compliance with applicable Federal standards. Employees will be notified of such changes as they occur.

Section 101: Definition of CPNI:

CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relations; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

From a practical perspective, CPNI includes a customer's personally identifiable information such as the phone numbers called by a consumer, the frequency duration, and timing of such calls (call detail information); and any services purchased by the customer (non-call detail information), such as call waiting. CPNI is any customer information that is obtained by TC because of the customer/carrier relationship. CPNI should be considered by employees as highly-sensitive personal information. The CPNI regulations apply to information of customers obtained by wireline, wireless, long distance, and Interconnected Voice over Internet Protocol (VoIP) service providers. By contrast, information that is available in a telephone directory is called "subscriber list information," and is not considered CPNI.

Section 102: Categories of Customer Information:

Federal law and regulations describe three general categories of customer information to which different levels of privacy protection and carrier obligations apply: (1) individually identifiable CPNI, (2) aggregate customer information, and (3) subscriber list information.

1. Individually identifiable “CPNI” was described in Section 101 of this document.
2. “Aggregate customer information” is collective data that relates to a group or category of services or customers from which individual customer identities and characteristics have been removed. Certain Federal regulations govern treatment of this information, and requests for such information shall be forwarded to the Regulatory Department for CPNI Compliance.
3. “Subscriber list information” is any information identifying the listed names of a carrier’s subscribers’ telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications, and that the carrier or an affiliate has published, caused to be published, or accepted for publishing in any directory format. Certain Federal Communications Commission (FCC) regulations govern treatment of this information. “aggregate customer information” and “subscriber list information” are not considered CPNI. The Company may from time-to-time use subscriber list information for marketing. *Requests for aggregate customer information and subscriber list information shall be forwarded to the Regulatory Department for CPNI Compliance.* *(Refer to Section 108 for information regarding the Contact of CPNI Compliance.)*

Section 103: Company Policy Regarding CPNI:

As described above, CPNI is information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of the Company, and that is available to the Company solely by virtue of the carrier-customer relations with our subscribers. CPNI includes information contained in the bills pertaining to telephone exchange service or telephone toll service received by our customers.

Telecommunications carriers have a federal legal duty to protect the confidentiality of their customers’ CPNI.

It is the policy of the Company to have security systems and procedures designed to protect CPNI form unauthorized disclosure and to comply with all Federal statutes and regulations regarding the use of CPNI.

The Company may use, disclose or permit access to CPNI for marketing purposes with the Company or its affiliates (subject to Federal statutes and regulations); however it is the current policy of the Company to avoid providing CPNI to any third party *except* where such disclosure is, in the Company’s view, necessary to protect the rights or property of the Company or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services, or to perform billing and collections services. The Company notes that when disclosing CPNI for billing and collection services, the Company has entered into appropriate confidentiality agreements with the entities with which the Company has contracted for such billing and collection services, as required by federal regulations, Additionally, the Company

may use, disclose, or permit access to CPNI to provide certain telemarketing, referral, or administrative services to a customer for the duration of a call that was initiated by the customer, if the customer approves of the use of the information to provide such services. *(Refer to Section 104 for additional explanation.)*

Section 104: Authorized Use of CPNI:

According to federal law, the Company has a general duty to protect the confidentiality of CPNI. In addition, federal law provides that a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances as explained below, unless the carrier has gone through the process described in the FCC's rules of obtaining customer approval to use or disclose their records through either the "opt-in" or "opt-out " approval method as prescribed by the FCC. In general, under the opt-in or opt-out rules, the carrier provides notice to the customer of his/her right to restrict access from use of, or disclosure of CPNI. Under the opt-in method, the customer must provide affirmative approval to the Company authorizing the access, use or disclosure of the customer's CPNI. Under the opt-out method, a customer's lack of response is considered approval.

Under federal regulations, the Company can permit access to and use of CPNI without going through the opt-in or opt-out customer approval process under the following circumstances:

- to provide or market service offerings that are among the categories of service to which the customer already subscribes (for example, the Company could use local service CPNI to market long distance offerings without customer approval, unless the customer also subscribed to long distance service from the Company
- to bill and collect for telecommunications services (subject to a confidentiality agreement when such billing and collection services are provided under contract between a third party and the Company);
- to protect the rights or property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;
- to provide any telemarketing of services, referrals, or administrative services for the duration of the call in response to an inbound call initiated by the customer, if the customer approves of the use of the CPNI for that purpose. In these instances, a customer can give oral approval (which is effectively a form of opt-in approval) subject to the requirements provided for in Section 64.2008(f) of the FCC's rules.
- to report violations of specific federal statutes relating to child pornography (42 U.S.C. 13032 requires providers of electronic communication service or remote computing service to report apparent violations of certain federal statutes involving child pornography to the CyberTipLine operated by the National Center for Missing and Exploited Children).

The Company can use CPNI derived from its provision of local exchange service or interexchange service, without customer approval, to market CPE and some information services which are: call answering, voice mail or messaging, voice storage and retrieval services, inside wiring installation and maintenance fax store and forward and protocol conversion. The Company can also use information derived fro the provision of non-telecommunications service, such as CPE or information services, to provide or market any telecommunications service.

It is the Company's policy to obtain approval to use, disclose or permit access to a customer's CPNI for marketing purposes through the opt-out method, in accordance with the FCC's rules. *(See Appendix A, Section 64.2008 for notice requirements).* When a customer denies approval for the use of their CPNI, the customer's records are noted. Opt-out notice must be sent every two years.

Customer Requests for CPNI:

Federal law also guarantees customers the right to obtain access to, and compel disclosure of, their CPNI. A telecommunications carrier is required to lease the CPNI to any person designated by the customer upon and "affirmative written request by the customer." *(Section 105 describes the Company's procedures when customer calls the Company to gain access to their CPNI.)*

Section 105: Procedures to Prevent Unauthorized Disclosure of CPNI:

In order to prevent the unauthorized or unlawful disclosure of CPNI, the Company has instituted the following procedures in accordance with Federal regulations.

CUSTOMER AUTHENTICATION

For customer-initiated incoming calls, CPNI is not discussed with a customer until the customer has been properly authenticated to ensure that the calling party is an authorized person on the account.

Call detail information is not discussed with a customer on a customer-initiated call unless the customer can provide a pre-established password, or the customer has sufficient details about the call(s) in question to address the customer service issue (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call), and can provide the information without assistance. If the customer is unable to provide a password, call detail information can by shared only by(1)calling the customer back at the telephone number of record(the telephone number associated with the underlying service - not a contact number); (2)mailing the information to the address of record (an address - postal or electronic - associated with the customer's account for at least 30 days); or (3) the customer coming to the office with a valid photo I.D.

For new customers, passwords and back-up questions and responses (to be used if a password is lost are forgotten) are determined when the customer places an order to

establish service. The passwords and back-up questions must not be based on readily available biographical or account information. (Readily available biographical information is information drawn from the customer's life history such as a social security number, mother's maiden name, home address or birth date. Account information includes the account number, telephone number, or amount of the last bill.) In the event a customer forgets both their password and response to back-up questions, or requests a new password, the customer must be authenticated by coming to the office and presenting a valid picture ID that matches the name on the account or call the Company from the telephone number of record. The Company representative will call the customer back at the telephone number of record.

Non-call detail information, such as billing or services provided, can be discussed after the customer is authenticated using standard procedures, such as personally-identifiable information noted on the account records (without the use of a password.)

BUSINESS CUSTOMER EXEMPTION

The customer authentication requirements may be exempt when the Company chooses to serve a business customer through a dedicated account representative as the primary contact, and address the Company's protection of CPNI in the customer's contract.

CUSTOMER NOTIFICATION OF ACCOUNT CHANGES

As an additional precaution to protect customers in the event that authentication protections may have been circumvented by unauthorized persons, customers are notified of certain account changes. Whenever a password, back-up means of authentication, online account or address of record is created or changed, the Company must immediately notify the customer by either mail to the address of record, or by voice mail to the telephone number of record. It is the Company's policy to mail a letter to the customer's address of record notifying the customer that a change has been made. If the change is to the address of record, the notification of the change will be mailed to the old address.

JOINT VENTURE PARTNER/INDEPENDENT CONTRACTOR RELATIONSHIPS

It is the Company's policy not to disclose or provide access to CPNI to Joint Venture Partners or Independent Contractors for marketing purposes. If in the future the Company decides to share customers' CPNI for marketing purposes, CPNI will be shared of only those customers who have given express consent(opt-in approval) to do so.

It is the Company's policy to enter into Non-Disclosure and Confidentiality Agreements with Independent Contractors such as billing vendors and equipment contractors that may have access to CPNI. A standard Confidentiality Agreement is included in Appendix B.

REQUESTS FOR CPNI FROM PERSONS OTHER THAN THE CUSTOMER

The following guidelines govern employee responses to requests for CPNI from persons other than the customer(such as a billing company or. law enforcement representative).

- A Company employee that receives a request for CPNI from a person other than the customer (Requesting Entity) shall obtain the name of the requester's employer, employer's contact information (including address and telephone number), and business purpose.

- The employee shall refer the request to the Regulatory Department for CPNI Compliance for review and authorization.

- The Company Regulatory Department for CPNI Compliance shall determine whether the customer whose CPNI is contemplated by the request has consented to use or disclosure of the CPNI. It is the policy of the Company not to use or disclose CPNI to Joint Venture partners or Independent Contractors for marketing. If in the future the Company decides to share CPNI with Joint Venture partners or Independent Contractors for marketing purposes, it will only be done when opt-in consent is received from the customer whose CPNI would be shared. If the customer has not consented to release of the CPNI, then CPNI may not be released unless the Requesting Entity has requested the CPNI pursuant to one of the following circumstances, subject to the conditions described below, which shall be evaluated by the Company Regulatory Department for CPNI Compliance:

1. The Requesting Entity has requested the CPNI in order to initiate, render, bill, and collect for telecommunications services. In such instances, the CPNI may be released only if the Company has entered into a Non-Disclosure and Confidentiality Agreement with that Requesting Entity.

2. The Requesting Entity has requested the CPNI in order to protect the rights or property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services. In this instance, the Company may use, disclose, or permit access to CPNI, either directly or indirectly through its agents. In such instances, the Company Regulatory Department of CPNI Compliance shall ensure that a release and warranty is executed with the Requesting Entity before the Company uses, discloses, or permits access to the CPNI.

3. Reporting violations of specific federal statutes relating to child pornography (42 U.S.C. §13032).

4. In the case of requests from law enforcement agencies, it must be determined that the proper subpoenas or other legal documents are in effect.

If the Requesting Entity's request for CPNI does not conform to the circumstances and conditions described above, then the CPNI shall not be released.

Section 106: Record-keeping Requirements:

The Company will maintain a record, electronically or in some other manner, of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. This record must include a description of each sales or marketing campaign; the specific CPNI that was used in the campaign; and, the products and services that were offered as part of the campaign. *This record must be retained for a minimum of one year.*

In the event the Company uses, discloses, or permits access to CPNI for its own or an affiliate's sales and marketing campaign, the Company will maintain a record, electronically or otherwise, of the following: a description of each sales or marketing campaign; the specific CPNI that was used in the campaign; and, the products and services that were offered as part of the campaign. *This record must be retained for a minimum of one year.*

Records of notification of a customer's right to restrict the use of, disclosure of, and access to that customer's CPNI, whether oral, written, or electronic, shall be maintained for at least one year.

Records of a customer's approval or disapproval to use, disclose, and access that customer's CPNI, whether oral, written, or electronic, shall be maintained for at least one year. The records of customer approval and disapproval for use of CPNI are maintained in a readily-available location that is consulted on an as-needed basis.

Sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval to access and use CPNI. A supervisory review process regarding compliance with the rules for outbound marketing situations is required, *and maintenance of records of Company compliance must be maintained for a minimum of one year.*

In the event of a breach (an occurrence when a person without authorization has intentionally gained access to, used, or disclosed CPNI), for a minimum of two years the Company shall maintain a record of any breaches discovered, notifications made to law enforcement agencies (U.S. Secret Service and Federal Bureau of Investigation), and notifications made to customers. The record must include, if available, dates of discovery and notifications, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Section 107: Security Systems to Protect CPNI:

The Company employs the following security measures to protect its data, including customer CPNI:

Unattended Computers:

It is the Company's policy that when a computer or other device from which CPNI can be accessed is unattended, employees must shut down or otherwise log off or electronically lock the system so access by an unauthorized person(s) is prevented.

Customer Paper Records:

It is the Company's policy that paper records containing confidential information be secured at all times when not in use by an authorized person, such as a customer service representative using paper records to discuss the account with the customer. In the event that a customer's record is no longer to be retained, it is the Company's policy that the record be shredded. Under no circumstances should customer records be discarded in the trash without shredding.

On-Line Access to Customer Accounts:

It is the Company's policy that its online systems be designed to protect customers' telecommunications service accounts from unauthorized access. Authentication processes are in place prior to allowing the customer online access to CPNI related to a telecommunications service account. Prior to such access, the customer is authenticated without the use of readily available biographical information, or account information. A customer cannot access his or her telecommunications account without a password, and

that password is not prompted by the Company asking for readily available biographical information or account information.

The system is set up to log off a party who has attempted to access the account by typing an invalid password after a pre-determined number of attempts. The Company has a back-up authentication process for customers in the event of a lost or forgotten password that does not rely on readily available biographical information or account information.

Section 108: Safeguards For Use of CPNI:

Federal regulations require the Company to implement safeguards for the use of CPNI. The Company has appointed a Director for CPNI Compliance to serve as the central point of contact for employees, agents (contractors, vendors, consultants, attorneys) and customers regarding the Company's CPNI responsibilities and questions related to CPNI policy. The Director for CPNI Compliance has the responsibility to investigate complaints of unauthorized release of CPNI, report any breaches to the appropriate law enforcement agencies; and maintain CPNI records in accordance with FCC rules. The Director for CPNI Compliance ensures that processes are in place to track customer complaints of unauthorized release of CPNI for each year, maintains records of CPNI breaches for at least two years, and supervises the training of all Company employees with access to CPNI.

All carriers are required by the FCC to have an officer, on an annual basis and as an agent of the carrier, sign and file with the FCC a compliance certification stating that the officer has personal knowledge that the Company has adequate operating procedures to ensure compliance with the FCC CPNI Rules. A sample certification is included in Appendix C to this document. In addition, the carrier must provide a statement accompanying the certification explaining how its operating procedures ensure that the carrier is or is not in compliance with the applicable Federal Rules. An explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI must also be included with this statement.

A sample accompanying statement to the CPNI compliance certification is included in Appendix D to this document.

The compliance certification and accompanying statement must be filed annually with the FCC's Enforcement Bureau by March 1 in EB Docket No.06-36 for data pertaining to the previous calendar year. A compliance certification and accompanying statement must be filed for each telecommunications entity.

Copies of the Company's annual certifications are maintained by the Company in compliance with its record-keeping policies.

Section 109: Disciplinary Process for Employee Misuse of CPNI:

The FCC requires that telecommunications carriers train their employees regarding when they are or are not authorized to use CPNI, and have an express disciplinary process in place. Although the FCC does not differentiate whether a violation of the CPNI rules is intentional or unintentional, they also do not prescribe specific disciplinary actions. The Company reserves the right to undertake disciplinary measures consistent with Company policy to address employee misuse of CPNI.

Disciplinary measures may call for any of our steps - verbal warning, written warning, suspension with or without pay, or termination of employment - depending upon the severity of the problem and number of occurrences. There may be circumstances when one or more of the steps are bypassed. For instance, an unintentional violation of the CPNI rules may result in the employee being reprimanded and retrained. For repeated unintentional violations, the employee may be suspended or terminated. In the case of an intentional violation, such as providing CPNI to third parties for financial gain or to harm the customer or company, the employee should be terminated.

The Company will ensure fair treatment of all employees and make certain that disciplinary actions are prompt, uniform, and impartial. The major purpose of any disciplinary action is to correct the problem, prevent recurrence, and prepare the employee for satisfactory service in the future.

Section 110: Documentation of CPNI Training:

This is to acknowledge that the Company employee named below has undergone Company-sponsored training regarding when CPNI use is authorized, and when CPNI is not authorized. The Company employee named below has read and understands the Company's policy and procedures regarding CPNI.

Documentation of CPNI Training

> *As an employee of Tularosa Communications (the Company), I have completed CPNI training, and have read and understand the Company's CPNI Policy and Procedures. I acknowledge that violations of the Company's Policy and Procedures regarding the use of CPNI and violations of FCC rules will be cause for disciplinary action by the Company and possible termination of employment.*

Employee _____

Date _____

Section 111: Notification of CPNI Security Breaches:

Federal regulations require that the Company notify law enforcement of any breach of its customers' CPNI. As defined by federal regulations, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

An employee who has knowledge of or suspects that a breach has occurred shall immediately notify his or her supervisor, whose responsibility it is to notify the Director of CPNI Compliance. Within seven (7) business days after reasonable determination of a breach, the Company is required to electronically notify the United States Secret Service (USSS) and the Federal Bureau of lnvestigation (FBI) through the FCC central reporting facility at http://www.fcc.gov/eb/cpni. Because some breaches might merit criminal investigation and require that the investigation remain confidential, customers are **not** to be notified or the breach disclosed to the public until seven (7) full business days after notification was made to the USSS and FBI. The investigating agency may delay public disclosure or customer notice of the breach for 30 days or longer if it determines that such notice would impede or compromise a criminal investigation or national security.

After notifying the law enforcement agencies and without any requests for delays from them, the Company is required to notify customers of a breach in their CPNI.

Circumstances may require that the Company notify customers or the public earlier in order to avoid immediate and irreparable harm; however, it will do so only after consultation with the relevant law enforcement agency. *See Section 106 - Record - Keeping Requirements pertaining to maintaining records of the breach.*

Section 112: Federal Communications Commission CPNI Rules:

The FCC's rules on CPNI are included in Appendix A of this document.

Section 113: Privacy Policy:

The Company's Privacy Policy is attached as Appendix E to this document.

Appendix A: FCC Rules on CPNI:

TITLE 47--
TELECOMMUNICATION
CHAPTER 1—FEDERAL
COMMUNICATIONS COMMISSION
PART64 MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Subpart U Customer Proprietary Network Information

Sec.64. 2001 Basis and purpose.

(a) Basis. The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.
(b) Purpose. The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended,47 U.S.C. 222.

Sec.64.2003 Definitions

Terms in this subpart have the following meanings:
(a) ***Account Information.*** "Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.
(b) ***Address of record.*** An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.
(c) ***Affiliate.*** The term "affiliate" has the same meaning given such term in section 3(1)of the Communications Act of 1934, as amended,47 U.S.C. 153(1).
(d) ***Call detail information.*** Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location or duration of any call.
(e)***Communications-related services.*** The term "communications- related services" means telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.
(f) ***Customer.*** A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.

(g) ***Customer proprietary network information(CPNI).*** The term "customer proprietary network information(CPNI)" has the same meaning given to such term in section 222(h)(l) of the Communications Act of 1934, as amended,47 U.S.C. 222(h)(l).
(h) ***Customer premises equipment(CPE).*** The term "customer premises equipment (CPE)" has the same meaning given to such term in section 3(14)of the Communications Act of 1934, as amended,47 U.S.C. 153(14).
(i) Information services typically provided by telecommunications carriers. The phrase "information services typically provided by telecommunications carriers" means only those information services (as defined in section 3(20) of the Communications Act of 1934, as amended,47 U.S.C.153(2) that are typically provided by telecommunications carriers, such as Internet access or voice mail services. Such phrase "information services typically provided by telecommunications carriers," as used in this subpart, shall not include retail consumer services provided using Internet websites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.
(ii) (j) ***Local exchange carrier(LEC).*** The term "local exchange carrier (LEC)" has the same meaning given to such term in section 3(26) of the Communications Act of 1934, as amended,47 U.S.C. 153(26).
(k) ***Opt-in approval.*** The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.
(l) ***Opt-out approval.*** The ten "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in Sec. 64.2009(d)(l) after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.
(m) ***Readily available biographical information.*** "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.
(n) ***Subscriber list information (SLI).*** The term "subscriber list information (SLI)" has the same meaning given to such term in section 222(h)(3) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(3).
(o)***Telecommunications carrier or carrier.*** The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended,47 U.S.C. 153(44). For the purposes of this Subpart, the term "telecommunications carrier" or "carrier" shall include an entity that provides" interconnected VoIP service" as that term is defined in section 9.3 of these rules.

(p) ***Telecommunications service.*** The term "telecommunications Service" has the same meaning given to such term in section 3(46) of the Communications Act of 1934, as amended,47 U.S.C. 153(46).
(q) ***Telephone number of record.*** The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."
(r) ***Valid photo ID.*** A "valid photo ID"is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

Sec.64.2005 Use of customer proprietary network information without customer approval.

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS)to which the customer already subscribes from the same carrier, without customer approval.
(1) If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.
(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except as provided in Sec. 64.2007(b).
(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from that carrier, unless that carrier has customer approval to do so, except as described in paragraph (c) of this section.
(1) A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s). A wireline carrier may use, disclose or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.
(2) A telecommunications carrier may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.
(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this paragraph(c).
(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.
(3) LECs, CMRS providers, and entities that provide interconnected VoIP services as that term is defined in section 9.3 of these rules, may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.
(d) A telecommunications carrier may use, disclose, or permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

Sec.64.2007 Approval required for use of customer proprietary network information.

(a)A telecommunications carrier may obtain approval through written, oral or electronic methods.
(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part.
(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.
(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.
(b)Use of Opt-Out and Opt-In Approval Processes.(1)A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents *and* its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section § 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

Sec.64.2008 Notice required for use of customer proprietary network information.

(a) Notification, Generally.(1)Prior to any solicitation for customer approval, a telecommunications carrier must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral, written or electronic, for at least one year.
(b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.
(c) Content of Notice. Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.
(I)The notification must state that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI.
(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.
(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.
(4) The notification must be comprehensible and must not be misleading.
(5)If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.
(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.
(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.
(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.
(9) The notification must state that any approval, or denial of approval for the use ofCPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.
(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.
(b) Notice Requirements Specific to Opt-Out. A telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph(f) of this section. The contents of any such notification must comply with the requirements of paragraph (c) of this section.
(1) Carriers must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may, in its discretion, provide for a longer period. Carriers must notify customers as to the applicable waiting period for a response before approval is assumed.
(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.
(2) Carriers using the opt-out mechanism must provide notices to their customers every two years.
(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:
(i) Carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;
(ii) Carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;
(iii) Opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice;
(iv) Carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail; and
(v) Telecommunications carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.
(c) Notice Requirements Specific to Opt-In. A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph(c) of this section.
(f) Notice Requirements Specific to One-Time Use of CPNI.(1)
Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.
(2) The contents of any such notification must comply with the requirements of paragraph(c)of this section, except that telecommunications carriers may omit any of the following notice provisions if not relevant to the limited use for which the carrier seeks CPNI:
(i) Carriers need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;
(ii) Carriers need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;
(iii) Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use; and
(iv) Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

Sec.64.2009 Safeguards required for use of customer proprietary network information.

(a)Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use ofCPNI.
(b)Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.
(c)All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI.The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.
(d)Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.
(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No.06-36, for data pertaining to the previous calendar year.

(f) Carriers must provide written notice within five business days to the Commission 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.
(1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.
(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

§ ***64.2010*** Safeguards on the disclosure of customer proprietary network information.

(a)*Safeguarding CPNI.* Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

(b) *Telephone access to CPNI.* Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph(e)of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or, by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) *Online access to CPNI.* A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph(e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

(d)*In-store access to CPNI.* A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

(e)*Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords.* To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information.Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(f) *Notification of account changes.* Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(g) *Business Customer Exemption.* Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

§ **64.2011** Notification of customer proprietary network information security breaches.

(a)A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph(b).
(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.
(1)Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (2) and (3).
(2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (1), in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by earners.
(c) Customer Notification. After a telecommunications carrier has completed the process of notifying law enforcement pursuant to paragraph (b) it shall notify its customers of a breach of those customers' CPNI.
(d) Recordkeeping. All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b), and notifications made to customers. The record must

include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.
(e)Definitions. As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.
(f)This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

APPENDIX B: Nondisclosure/Confidentiality Agreement

TULAROSA BASIN TELEPHONE COMPANY, INC. (
Customer Proprietary Network Information (CPNI)
Non-Disclosure Agreement

This Customer Proprietary Network Information (CPNI) Non-Disclosure Agreement (this "Agreement") is entered into and is effective as of_____, 2024 (the "Effective Date"), by and between Tularosa Basin Telephone Company, Inc.(“TBTC”), a New Mexico Corporation whose address is 503 St. Francis Drive, Tularosa, NM 88352 and _____(Insert Recipient Company Name)("___")(Insert Abbreviated Recipient Company Name) a _____(Insert State Name) Corporation whose address is (Insert Recipient Company Address) (collectively, the "Parties").

WHEREAS, TBTC plans to provide ___(Insert Abbreviated Recipient Company Name) access to certain CPNI records of its customers, solely for the intended purposes as established herein; and

WHEREAS, the CPNI records of TBTC customers must be treated as highly confidential information, subject to the provisions of applicable federal statutes and regulations (collectively, "Confidential Information"); and

WHEREAS, both parties desire to reach an agreement whereby any CPNI of TBTC customers that _____(Insert Abbreviated Recipient Company Name) may be provided by TBTC for the limited purposes established in this agreement shall be protected by _____(Insert Abbreviated Recipient Company Name) from any disclosure or use, both internal and external to _____(Insert Abbreviated Recipient Company Name) and its affiliates, which is not specifically authorized as Approved Use under the terms of this Agreement.

NOW,THEREFORE, in consideration of the mutual promises and covenants contained herein, TBTC and (Insert Abbreviated Recipient Company Name) agree as follows:

1. Confidential Information: Means of Disclosure: *Exclusions*.
(a) TBTC, as "Disclosing Party," plans to provide access to (Insert Abbreviated Recipient Company Name), as "Recipient," certain Confidential Information in the form of CPNI records of its customers. This agreement is for the sole purpose of protecting data where Disclosing Party, in its sole discretion, elects to provide such data.
(b) All disclosures of information by the Disclosing Party to the Recipient pursuant to this Agreement shall be made by or under the supervision of the "Principal Contact(s)." The Principal Contacts for the parties are identified at the end of this Agreement. Each party may change its Principal Contact at any time and from time to time during the term

of this Agreement by notifying the Principal Contact of the other party in writing at the designated address.
(c) CPNI is considered to be Confidential Information and shall only be disclosed in accordance with this agreement.
(d) Recipient agrees to indemnify, defend and hold harmless the Disclosing Party from and against all losses, claims, demands, damages, costs, expenses, suits or other actions, or any liability whatsoever related to the disclosure by the Recipient of the CPNI provided to it by the Disclosing Party, including, but not limited to, settlements, fines, penalties, forfeitures, costs, expenses of investigation and defense and attorneys' fees arising from such disclosure. The indemnification, defense and hold harmless obligation as provided for herein shall be conditioned upon the Disclosing Party notifying the Recipient of any action taken against the Disclosing Party. Once such notification is made, the Recipient shall agree to work with the Disclosing Party's chosen counsel in defending any such action, and the Recipient may engage separate legal counsel only at its sole cost and expense. The Disclosing Party and Recipient shall work at all time in the defense of such action; provided, however, that the Disclosing Party shall retain the sole decision as to whether to settle or consent to any judgment pertaining to any such action.

2. Confidentiality Obligations.
(a) Recipient shall use commercially reasonable efforts to protect the confidentiality of the Confidential Information it receives from the Disclosing Party, at least equivalent to the degree of care that _(Insert Abbreviated Recipient Company Name) uses in its own business to protect its own similar Confidential Information, but in no event shall the degree of care be less than is reasonably required to effectuate the purpose of this Agreement. In particular, these efforts include restricting access to the Confidential Information to those individuals within _____’s (Insert Abbreviated Recipient Company Name) organization directly involved in performing the authorized use(s) of the Confidential Information, implementing procedures for safekeeping of writings, documents, and other media containing such Confidential Information, systematic use and enforcement of confidentiality agreements with all personnel who may have access to the Confidential Information, and implementing procedures for shredding or similar controlled disposal of materials that may contain such Confidential Information.
(b) Recipient may use the Confidential Information only for the *Approved Use* set forth herein. Recipient expressly agrees and acknowledges that the Confidential Information shall not be used for any other purpose, including but not limited to: marketing and marketing-related purposes, sales purposes, information gathering purposes, and strategic planning purposes.
(c) Recipient may provide the Confidential Information it receives from the Disclosing Party only to persons who (1) have a "need to know" such Confidential Information in order to enable Recipient to use such Confidential Information for such purposes and (2) are legally bound to use and disclose such Confidential Information for no other purpose. Recipient may provide the Confidential Information it receives from the Disclosing Party only to employees, contractors, or consultants of Recipient who (1) are directly assigned to participate in the projects or tasks for which the Confidential

Information is authorized by Disclosing Party, (2) have a "need to know" such Confidential Information to enable them to perform their responsibilities relating to such

projects or tasks, and (3) are subject to legally binding confidentiality obligations relating to the use and disclosure of such Confidential Information at least as restrictive as those herein.
(d) Recipient may, in addition, use or disclose Confidential Information if: (1) required by any request or order of any government authority, provided that Recipient shall first attempt to notify Disclosing Party of such requirement and, to the extent reasonable, permit the Disclosing Party to contest such requirement; (2) otherwise required by law. (e) Recipient shall notify Disclosing Party immediately in the event of loss or compromise of any Confidential Information received from the Disclosing Party.

3. Approved Use of Confidential Information. The Recipient agrees that it intends to use the CPNI records provided by Disclosing Party only for the purpose of _____ _____
Any other use of the CPNI records provided by Disclosing Party by Recipient is not in accordance with this agreement and is considered a breach of this agreement.

4. Destruction of Confidential Information. Recipient agrees to destroy all copies of any media or materials containing Confidential Information of Disclosing Party, including but not limited to all computer programs, documentation, notes, plans, drawings, and copies thereof immediately after such Confidential Information has been used for its authorized purpose. Notwithstanding the above, *Recipient may, if it so notifies Disclosing Party, retain a limited number of copies for a maximum of two years from the date provided for archival purposes only for reference with respect to the prior dealings between the parties.* Additionally, a Party may retain such information as required to comply with court or regulatory agency imposed retention obligations.

5. Term and Termination. The term of this Agreement shall commence on the date of this Agreement and shall end three (3) years after such date (the "Initial Term"). Thereafter, this Agreement shall be automatically renewed on a month-to-month basis (the "Renewal Periods"). At any time during the initial Term or the Renewal Periods, either party may terminate this Agreement with thirty (30) days prior written notice to the other party. However, termination will not relieve __(Insert Abbreviated Recipient Company Name) of its obligations of confidentiality and non-use arising under this Agreement.

6. No Implied License. No rights or licenses under copyright, patent or trademark of the Disclosing Party are granted or implied by either a confidential or non-confidential disclosure, except that Recipient may make a reasonable number of copies of documents in order to carry out an Approved Use of the Confidential Information as authorized by this Agreement.

7. Relief. The Parties agree that if Recipient were to breach any provisions of this Agreement, Disclosing Party or the affected customers of TBTC, whose CPNI records were provided under this Agreement, may be irreparably injured by a disclosure in breach of this Agreement. The parties further agree that TBTC or the affected customers of TBTC will be entitled to seek equitable relief, including, but not limited to, injunctive and other equitable relief and specific performance, in the event of any breach or threatened breach of the confidentiality provisions of this Agreement. Such remedies will not be deemed to be the exclusive remedies for a breach of this Agreement, but will be in addition to all other remedies available at law or in equity.

8. Affiliates. References to TBTC and to __(Insert Abbreviated Recipient Company Name) include each party's applicable Affiliates. An "Affiliate" means any business organization, foreign or domestic, at least 35% of whose capital, assets, voting stock, profits interests or similar participation rights is owned or controlled, directly or indirectly, by a party.

9. No Assignment. Except as expressly permitted otherwise by this Agreement, the rights and benefits of this Agreement may not be assigned by (Insert Abbreviated Recipient Company Name).

10. Miscellaneous. This Agreement constitutes the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous oral or written agreements concerning such Confidential Information. This Agreement may not be amended except by the written agreement signed by authorized representatives of both parties. This Agreement will be governed by and construed in accordance with the laws of the State of New Mexico.

Understood and Agreed:

Tularosa Basin Telephone Company, Inc.

By: _____
Name: _____
Title: _____

_____
(DATE)

PRINCIPAL CONTACT INFO:
Name: _____
Title: _____
Email: _____
Voice: _____
Fax: _____

_____
(Recipient Company Name)

By: _____
Name: _____
Title: _____

_____
(DATE)

PRINICPAL CONTACT INFO:
Name: _____
Title: _____
Email: _____
Voice: _____
Fax: _____

APPENDIX C: CPNI Certification to FCC

Annual 47 C.F.R. 64.2009(a) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [year] covering the prior calendar year [insert year]

1. Date filed: [date]

2. Name of company(s) covered by this certification: [company]

3. Form 499 Filer ID: [provide ID(s)]

4. Name of signatory: [name]

5. Title of signatory: [title]

6. Certification:

I, *[name of officer signing certification},* 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/is not]* in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules [attach accompanying statement].

The company*[has/has not]* taken any 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. *[NOTE:If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]*

The company [has/has not]received any customer complaints in the past year concerning the unauthorized release of CPNI.*[NOTE: If you reply in the affirmative, provide a summary of such complaints.This summary must include the number of complaints, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]*

The company represents and warrants hat 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 _____
[signature of an officer, as agent of the carrier]

APPENDIX D: Accompanying Statement of Certificate of Compliance

TULAROSA BASIN TELEPHONE COMPANY
2024 Annual Statement of FCC CPNI Rule Compliance

This statement accompanies the 2024 Customer Proprietary Network Information ("CPNI") Certification for the above listed company as required by Section 64.2009(e) of the Federal Communications Commission's (“FCC's") rules, for the purpose of explaining how the operating procedures of the Company ensure compliance with Part 64, Subpart U of the FCC's rules. See C.F.R. § 64.201 et. seq.

Identification of CPNI

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 Section 64.2003(g) and Section 222(f)(l) of the Communications Act of 1934 as amended (47 U.S.C. § 222(f)(l)).

Identification of Services Affected by CPNI Rules

The Company has established procedures and trained employees to recognize the different types of telecommunications and non-telecommunication services that affect how the Company uses CPNI.

Identification of Permissible Use of CPNI without Customer Authorization

The Company has established procedures and trained employees having access to, or occasion to use CPNI, to identify uses of CPNI not requiring customer authorization under Section 64.2005.

Identification of Use of CPNI Requiring Customer Authorization

The Company has established procedures and trained employees having access to, or occasion to use CPNI, to identify uses of CPNI requiring customer authorization under Section 64.2007.

Customer Notification and Authorization Process

The Company has established procedures and trained employees responsible for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval requirements under Section 64.2008.

Record of Customer CPNI Approval/Non-Approval

The Company has sufficient systems in place for maintaining readily accessible record of whether and how a customer responds to approval to use CPNI for marketing purposes as required by Section 64.2009(a).

Procedures Protecting Against Disclosure of CPNI

The Company implemented procedures for compliance with new Section 64.2010 including, but not limited to the following:*

Authentication of customers before disclosing CPNI on customer-initiated telephone contacts or business office visits.

The Company has implemented procedures to notify customers of account changes.

* The Company does not provide customers with on-line access to customer account information.

Actions Taken Against Data Brokers and Responses to Customer Complaints

Pursuant to Section 64.2009, the Company has not taken any action against data brokers and has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Disciplinary Process

The Company has in place a disciplinary process to address any unauthorized use of CPNI where the circumstances indicate authorization is required under Section 64.2006(b).

Supervisory Review Process for Outbound Marketing

The Company currently does not utilize CPNI for outbound marketing. Before undertaking the use of CPNI for outbound marketing purposes, the Company will establish a supervisory review process to ensure compliance with Section 64.2009(d).

Procedures for Notifying Law Enforcement of CPNI Security Breaches

The Company has adopted procedures to comply with Section 64.2011 for notifying law enforcement of CPNI security breaches, together with the related recordkeeping and deferred notification to customers.

APPENDIX E: Privacy Policy

PRIVACY POLICY of
TULAROSA COMMUNICATIONS

Our Commitment: Respect & Protect Our Customer's Privacy

Your privacy is important to us. TC (the Company) respects and protects the privacy of our customers. We carefully ensure the confidentiality of each customer's telephone account and calling information. Our employees are educated about their obligation to safeguard customer information and telephone calls, and are held accountable for any failure to meet their obligations.

The Information We Obtain and How We Use It

TC obtains information about customers that helps us provide service. This information is used for business purposes only. For example, we need to know your name, address, and the services you buy from us for billing purposes and to better serve you when you contact our service representatives about your account. It may also be beneficial for us to know about your telephone bill, your calling patterns, and whether you have special needs, so that we can offer you the most effective services for your needs when you contact us.

We publish and distribute directories in print. Customer names, addresses and telephone numbers are included in these directories without restriction to their use. TC is required by law to provide customer names, addresses and telephone numbers to unaffiliated directory publishers and directory assistance providers for their use in creating directories and offering directory assistance.

Information typically available from details on a customer's monthly telephone bill that has been obtained in the normal course of providing telephone service is known as Customer Proprietary Network Information (CPNI). CPNI might include the type of line, technical characteristics, class of service, current telephone charges, local and long distance billing records, directory assistance charges, usage data and calling patterns. TC does not sell CPNI in any form, including billing records, types of service, and calling habits to third parties. We do not use CPNI for marketing purposes unless we have your approval, nor do we provide CPNI to any third party or affiliate, except as required by law or in certain normal courses of business, as explained below.

- When you dial 911, information about your location may be automatically transmitted to a public safety agency.
- Certain information about your long distance calls is transmitted to your billing company for billing purposes.
- As necessary, TC must disclose information to comply with court orders or subpoenas. We will also share information to protect our rights or property and to

protect use of our services and other carriers from fraudulent, abusive or unlawful use of services.

- TC may also use third parties or contractors to do work for the Company, such as billing services.These third party contractors have the same obligations as our regular employees concerning the confidentiality of our customer information. In cases where it is necessary to provide CPNI to a third party or affiliate, TC requires that those parties sign an agreement that they will protect the confidentiality of our customers' CPNI.
- We may, where permitted by law, provide personal information to credit bureaus, or provide information and/or sell receivables to collection agencies, to obtain payment for our products and services. We will enter into with the company or companies with whom we deal in this regard appropriate confidentiality agreements.

Your Telephone Account Information Rights

Under Federal Law, you have the right to, and we have the duty to protect the confidentiality of your telecommunications service information. Under Federal Communication Commission rules, without further authorization from you, we can use CPNI to offer you services of the type you already purchase from us, or we may share CPNI with our affiliates that offer different categories of service, if they already have an existing service relationship with you. TC offers local telephone service (dial tone), long distance, Internet and Managed Services.

If TC should decide to use or provide CPNI to offer you services that may be different from the type of services you currently buy from us, you will be notified in advance. You will then have the opportunity to tell us you do not want us to use your CPNI for that purpose.

Services to Enhance Your Privacy

You may choose to have a non-published number that will eliminate your telephone number from TC's printed directory or directory assistance. The non-published number will not be provided to other directory publishers or directory assistance providers.

You may choose to have a non-listed number. Non-listed numbers are not available in TC's printed directory, but are publicly available through directory assistance. These numbers may be provided to other directory assistance providers.

You may also choose to exclude partial or all address information from your listings.

Privacy management services, such as Caller ID and Caller ID blocking, are available to customers.

If you have questions or concerns regarding this statement you may contact us by calling our business office at 575-585-2700 or write to us at PO Box 550, Tularosa, NM 88352.