

CHEYENNE RIVER SIOUX TRIBE TELEPHONE AUTHORITY

GENERAL COMPANY POLICY

POLICY BULLETIN #5.19B

SUBJECT: PRIVACY AND CUSTOMER SECURITY

POLICY: C.R.S.T. Telephone Authority is committed to assuring strong and meaningful customer privacy protection in an era of rapidly changing communications technology and applications.

Our goal is simple: balance our customers' concerns about privacy with their interest in receiving quality service and useful new products. C.R.S.T. Telephone Authority is committed to informing customers, and giving customers choices, about how we use information about them. Above all, this Policy is designed to ensure that C.R.S.T. Telephone Authority will respect a customer's desire for privacy. If you have any questions about our policy, please contact us at crstta@lakotanetwork.com or 605-964-2600.

This Policy applies to our use of "individual customer information," that is, information about specific customers. Information that does not reveal a customer's identity is not individual customer information. For example, "aggregated information," such as the number of customers to access a Web site in a particular day, does not raise privacy concerns and is not covered by this policy.

Information Collection and Use

C.R.S.T. Telephone Authority obtains and uses individual customer information for business purposes only. We obtain information about our customers that helps to provide them with C.R.S.T. Telephone Authority services. This information may also be used to protect customers, employees and property against fraud, theft or abuse; to conduct industry or consumer surveys; and to maintain good customer relations.

Customers have many opportunities to control how we use their individual information to introduce them to new products and services. For example, C.R.S.T. Telephone Authority will not call customers who have expressed to us a preference not to be called for marketing purposes. Customers can also have their names removed from direct mail lists that we use. The same will be true for email if C.R.S.T. Telephone Authority decides to use email to send new product information to its customers.

However, we do use individual customer information internally for our own general marketing and planning purposes-so that we can, for example, develop, test and market new products and services that meet the needs of our customers. Unless we have your consent, such information is combined into aggregations that do not include individual customer identities. Under certain circumstances, we are required by law to disclose the aggregated information to other companies, but in such cases customer identities are not included.

Disclosure of Individual Customer Information

C.R.S.T. Telephone Authority enables customers to control how and if C.R.S.T. Telephone Authority discloses individual information about them to other persons or entities, except as required by law or to protect the safety of customers, employees or property. For example, if C.R.S.T. Telephone Authority is served with valid legal process for customer identification, we may be required to release this information. In addition, under certain circumstances, we share customer information with other carriers and with law enforcement to prevent and investigate fraud and other unlawful use of communications services.

Subject to legal and safety exceptions, C.R.S.T. Telephone Authority will share individual customer information only with persons or entities outside the company when the customer has consented, or when we have advised the customer of the opportunity to "opt-out" (to choose not to have the information disclosed). We are required to provide directory publishers with listings information-name, address and phone number-for purposes of publishing and delivering directories. Persons can ask to not be published in directors and/or Directory Assistance (there may be a cost associated with such action). However, if C.R.S.T. Telephone Authority enters into a merger, acquisition, or sale of all or a portion of its assets, a customer's personally identifiable information will, in most instances, be transferred as a part of the transaction. In addition, we may, where permitted by law, provide information to credit bureaus, or provide information and/or sell receivables to collection agencies, to obtain payment for C.R.S.T. Telephone Authority billed products and services.

Information Management and Security

All C.R.S.T. Telephone Authority employees are responsible for safeguarding individual customer communications and information. C.R.S.T. Telephone Authority requires its personnel to be aware of and protect the privacy of all forms of customer communications-whether they are voice, data or image

transmissions-as well as individual customer records. C.R.S.T. Telephone Authority makes clear that employees who fail to follow this Privacy and Customer Security Policy will face disciplinary action, which can include dismissal. All employees are trained regarding their responsibilities to safeguard customer privacy.

C.R.S.T. Telephone Authority strives to ensure that information we have about our customers is accurate, secure and confidential, and to ensure that our employees comply with our privacy policy. We never tamper with, intrude upon or disclose the existence or contents of any communication or transmission, except as required by law or the proper management of our

network. Access to databases containing customer information is limited to employees who need it to perform their jobs-and they follow strict guidelines when handling that information. We use safeguards to increase data accuracy and to identify and authenticate the sources of customer information. We use locks and physical security measures, sign-on and password control procedures, internal auditing techniques and other types of security as appropriate for the information stored to protect against unauthorized use of terminals and entry into our data systems.

C.R.S.T. Telephone Authority requires that records be safeguarded from loss, theft, unauthorized disclosure, and accidental destruction. In addition, sensitive, confidential, or proprietary records must be protected and maintained in a secure environment. It is our policy to destroy records containing sensitive, confidential, or proprietary information in a secure manner. Hard copy confidential, proprietary, or sensitive documents must be made unreadable before disposition or recycling, and electronic media must be destroyed using methods that prevent access to information stored in that type of media. Just as employees would report stolen property, employees must report missing records and suspicious incidents involving records.

We encourage our employees to be proactive in implementing and enforcing the C.R.S.T. Telephone Authority Privacy and Customer Security Policy. If employees become aware of practices that raise privacy concerns, they are encouraged to report them to their supervisors.

Compliance with Laws and Public Policy Participation

C.R.S.T. Telephone Authority complies with all applicable privacy laws and regulations. Customer and policymaker perceptions of privacy have changed over time and will continue to do so. Changes in technology can also alter what is appropriate in protecting privacy. Laws may change accordingly. We will regularly examine-and update, if necessary-the C.R.S.T. Telephone Authority Privacy and Customer Security Policy.

What if I do not consent?

You can contact us at 605-964-2600. You will not receive company information from us at that point. You may miss the opportunity to learn of new, innovative service proposals, new packaging that could reduce your monthly bill and other information that keeps you informed of the happenings of C.R.S.T. Telephone Authority.

This policy supersedes and cancels all similar policies prior to this date.

DATE ADOPTED: November 23, 2016

DATE REVISED: _____

DATE REVIEWED: _____