CISP CPNI Policy for CISP

Customer Proprietary Network Information Policy

Community ISP, Inc. (CISP) is committed to maintaining the privacy of its customers. In addition to protecting your personal information as outlined in CISP's Privacy Policy, we are obliged to give additional protections to certain information about how you use your services. However, that information can help us customize and improve services we offer you.

In this section, we describe what information we protect and how we protect it.

CPNI PROTECTIONS

As a customer of our services, you have the right, and CISP has a duty, under federal law, to protect the confidentiality of certain types of services, including: (1) information about the quantity, technical configuration, type, destination, location, and amount of your use of your services, and (2) information contained on your telephone bill concerning your services you receive. That information, when matched to your name, address, and telephone number is known as "Customer Proprietary Network Information," or "CPNI" for short. Examples of CPNI include information typically available from telephone-related details on your monthly bill, technical information, type of service, current telephone charges, long distance and local service billing records, directory assistance charges, usage data and calling patterns.

CPNI does not include things like customer name, address, or telephone number; aggregate information or data that is not specific to a single customer; customer premises equipment; and Internet access services.

Unless CISP obtains your approval, CISP may not use this CPNI to market products and services to you other than for services you currently purchase. Customer proprietary network information ("CPNI") is information related to the quantity, technical configuration, type, destination, location, and the amount of telecommunications a customer uses that CISP has access to by virtue of the customer-provider relationship. CPNI does not include the Customer name, address and telephone number, nor does it include Internet access services.

APPROVAL

From time to time, CISP would like to use the CPNI information it has on file to provide you with information about CISP's communications-related products and services or special promotions. CISP's use of CPNI may also enhance its ability to offer products and services tailored to your specific needs. Accordingly, CISP would like your approval so that CISP may use this CPNI to let you know about communications-related services other than those to which Customer currently subscribes that CISP believes may be of interest to Customer. **IF Y0U APPROVE, YOU DO NOT HAVE TO TAKE ANY ACTION.**

However, you do have the right to restrict our use of your **CPNI. YOU MAY DENY OR WITHDRAW CISP's RIGHT TO USE YOUR CPNI AT ANY TIME BY CALLING 419-724-3547.** If you deny or restrict your approval for CISP to use your CPNI, you will suffer no effect, now or in the future, on how CISP provides any services to which you subscribe. Any denial or restriction of your approval remains valid until your services are discontinued or you affirmatively revoke or limit such approval or denial.

In some instances, CISP will want to share your CPNI with its independent contractors and joint venture partners in order to provide you with information about CISP's communications-related products and services or special promotions. Prior to sharing your CPNI with its independent contractors or joint venture partners, CISP will obtain written permission from you to do so.

CUSTOMER AUTHENTICATION

Federal privacy rules require CISP to authenticate the identity of its customer prior to disclosing CPNI. Customers calling CISP's customer service center can discuss their services and billings with a CISP representative once that representative had verified the caller's identity. There are three methods by which CISP will conduct customer authentication:

by having the Customer provide a pre-established password and/or PIN;
by calling the Customer back at the telephone number associated with the services purchased; or
by mailing the requested documents to the Customer's address of record.

Passwords and/or PINs may not be any portion of the Customer's social security number, mother's maiden name, amount or telephone number associated with the Customer's account or any pet name. In the event the Customer fails to remember their password and/or PIN, CISP will ask the Customer a series of questions known only to the Customer and CISP in order to authenticate the Customer. In such an instance, the Customer will then establish a new password/PIN associated with their account.

NOTIFICATIONS OF CERTAIN ACCOUNT CHANGES

CISP will be notifying customers of certain account changes. For example, whenever an online account is created or changed, or a password or other form of authentication (such as a "secret question and answer") is created or changed, CISP will notify the account holder. Additionally, after an account has been established, when a customer's address (whether postal or e-mail) changes or is added to an account, CISP will send a notification. These notifications may be sent to a postal or e-mail address, or by telephone, voicemail or text message.

DISCLOSURE OF CPNI

CISP may disclose CPNI in the following circumstances:

When the Customer has approved use of their CPNI for CISP or CISP and its joint venture partners and independent contractors (as the case may be) sales or marketing purposes.
When disclosure is required by law or court order.
To protect the rights and property of CISP or to protect Customers and other carriers from fraudulent, abusive, or unlawful use of services.
When a carrier requests to know whether a Customer has a preferred interexchange carrier (PIC) freeze on their account.
For directory listing services.
To provide the services to the Customer, including assisting the Customer with troubles associated with their services.
To bill the Customer for services.

PROTECTING CPNI

CISP uses numerous methods to protect your CPNI. This includes software enhancements that identify whether a Customer has approved use of its CPNI. Further, all CISP employees are trained on the how CPNI is to be protected and when it may or may not be disclosed. All marketing campaigns are reviewed by a CISP supervisory committee to ensure that all such campaigns comply with applicable CPNI rules.

CISP maintains records of its own and its joint venture partners and/or independent contractors (if applicable) sales and marketing campaigns that utilize Customer CPNI. Included in this, is a description of the specific CPNI that was used in such sales or marketing campaigns. CISP also keeps records of all instances in which CPNI is disclosed to third parties or where third parties were allowed access to Customer CPNI.

CISP will not release CPNI during customer-initiated telephone contact without first authenticating the Customer's identity in the manner set-forth herein. Violation of this CPNI policy by any CISP employee will result in disciplinary action against that employee as set-forth in CISP' Employee Manual.

BREACH OF CPNI PRIVACY

In the event CISP experiences a privacy breach and CPNI is disclosed to unauthorized persons, federal rules require CISP to report such breaches to law enforcement. Specifically, CISP will notify law enforcement no later than seven (7) business days after a reasonable determination that such breach has occurred by sending electronic notification through a central reporting facility to the United States Secret Service and the FBI. A link to the reporting facility can be found at: www.fcc.gov/eb/cpni. CISP cannot inform its Customers of the CPNI breach until at least seven (7) days after notification has been sent to law enforcement, unless the law enforcement agent tells the carrier to postpone disclosure pending investigation. Additionally, CISP is required to maintain records of any discovered breaches, the date that CISP discovered the breach, the date carriers notified law enforcement and copies of the notifications to law enforcement, a detailed description of the CPNI breach, including the circumstances of the breach, and law enforcement's response (if any) to the reported breach. CISP will retain these records for a period of not less than two (2) years.

NOTIFICATION OF CHANGES TO THIS POLICY

If we change this CPNI Policy, we will post those changes on http://cisp.com/about/cpni/ or in other places we deem appropriate, so that you can be aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If you decide to continue receiving your services after we make any changes to this the CPNI Policy, you shall be deemed to have given express consent to the changes in the revised policy.(such as a "secret question and answer") is created or changed, CISP will notify the account holder. Additionally, after an account has been established, when a customer's address (whether postal or e-mail) changes or is added to an account, CISP will send a notification. These notifications may be sent to a postal or e-mail address, or by telephone, voicemail or text message.

DISCLOSURE OF CPNI

CISP may disclose CPNI in the following circumstances:

When the Customer has approved use of their CPNI for CISP or CISP and its joint venture partners and independent contractors (as the case may be) sales or marketing purposes.
When disclosure is required by law or court order.
To protect the rights and property of CISP or to protect Customers and other carriers from fraudulent, abusive, or unlawful use of services.
When a carrier requests to know whether a Customer has a preferred interexchange carrier (PIC) freeze on their account.
For directory listing services.
To provide the services to the Customer, including assisting the Customer with troubles associated with their services.
To bill the Customer for services.

PROTECTING CPNI

CISP uses numerous methods to protect your CPNI. This includes software enhancements that identify whether a Customer has approved use of its CPNI. Further, all CISP employees are trained on the how CPNI is to be protected and when it may or may not be disclosed. All marketing campaigns are reviewed by a CISP supervisory committee to ensure that all such campaigns comply with applicable CPNI rules.

CISP maintains records of its own and its joint venture partners and/or independent contractors (if applicable) sales and marketing campaigns that utilize Customer CPNI. Included in this, is a description of the specific CPNI that was used in such sales or marketing campaigns. CISP also keeps records of all instances in which CPNI is disclosed to third parties or where third parties were allowed access to Customer CPNI.

CISP will not release CPNI during customer-initiated telephone contact without first authenticating the Customer's identity in the manner set-forth herein. Violation of this CPNI policy by any CISP employee will result in disciplinary action against that employee as set-forth in CISP' Employee Manual.

BREACH OF CPNI PRIVACY

In the event CISP experiences a privacy breach and CPNI is disclosed to unauthorized persons, federal rules require CISP to report such breaches to law enforcement. Specifically, CISP will notify law enforcement no later than seven (7) business days after a reasonable determination that such breach has occurred by sending electronic notification through a central reporting facility to the United States Secret Service and the FBI. A link to the reporting facility can be found at: www.fcc.gov/eb/cpni. CISP cannot inform its Customers of the CPNI breach until at least seven (7) days after notification has been sent to law enforcement, unless the law enforcement agent tells the carrier to postpone disclosure pending investigation. Additionally, CISP is required to maintain records of any discovered breaches, the date that CISP discovered the breach, the date carriers notified law enforcement and copies of the notifications to law enforcement, a detailed description of the CPNI breach, including the circumstances of the breach, and law enforcement's response (if any) to the reported breach. CISP will retain these records for a period of not less than two (2) years.

NOTIFICATION OF CHANGES TO THIS POLICY

If we change this CPNI Policy, we will post those changes on http://cisp.com/about/cpni/ or in other places we deem appropriate, so that you can be aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If you decide to continue receiving your services after we make any changes to this the CPNI Policy, you shall be deemed to have given express consent to the changes in the revised policy.