

ZIRRUS - Privacy Information

As a customer of Zirrus, you are entitled to know what we do with personal information about you that we receive. We consider our treatment of such information to be a part of the trust you place in us by using our Voice, Video, Broadband, and Internet Services. We provide this notice to better answer questions you may have, but our basic privacy policy remains the same. We keep only the personal information of our customers that is needed to provide our services, treat it as private, use it only for what we offer you, do not sell it to others, work to keep it secure and destroy it when no longer needed. While we cannot cover here every situation where your personal information may be affected, we have included those we believe are of most interest.

By law, we tell you annually about our privacy policy, and you can find additional and updated information at any time by visiting our website at (www.zirrus.com). You can learn more about your privacy rights by visiting the websites of the Federal Trade Commission, (www.ftc.gov), and the Federal Communications Commission (www.fcc.gov). If you receive your bills electronically, this notice will be sent to you similarly. If you cannot print an electronic copy of this notice, please contact us at (cstservice@Zirrus.com).

INFORMATION WE COLLECT

Personally Identifiable Information – In providing services to you, we obtain certain “personally identifiable information”, that is, information that identifies you individually (“your information”). Your information may include: name, service address, billing address, telephone number(s), social security number, driver’s license number, premium services you have selected, demographic information, user ID(s), password(s), email address(es), correspondence and communications records. We maintain customer information concerning credit, billing and payment, security deposits, maintenance and repair, equipment and services provided and other service-related functions. In providing our services, we may also collect information about your video equipment, phone system(s), computer hardware and software, modem(s), router(s), settings and other preferences to aid in customer support.

It is our policy to collect only the personal information needed to provide the services we offer with the quality you desire and deserve. It is also our policy to keep that information secure and to retain it only as long as needed for our business relationship or as the law may require. We take reasonable precaution to identify you or your authorized representative when we receive an inquiry on your account. We also take reasonable steps to protect your information from unauthorized access.

We sometimes collect personal information for special reasons, such as in surveys or registering at our Web sites. In these instances, you will be notified before it is collected, told how it will be used and may elect not to participate.

Internet Services – Like most Internet service providers, we automatically collect certain general information concerning your use, such as the Internet Protocol (IP) addresses assigned (an identifier assigned to your computer while online), bandwidth used, system and connection performance, browsers used, dates and times of access, and Internet resource requests, including requests to access web pages. We do not store online messages sent and received unless left in your Zirrus Internet account file. Since we cannot control Web sites or Internet services provided by third parties, we recommend that you review the terms of service and privacy policies of those Web sites and services. You can find more detailed information concerning our Online Privacy Policy on our website at www.zirrus.com.

Voice Services – We provide telephone services by traditional “switched” technology. We do not listen to or record your calls unless it is absolutely necessary while troubleshooting system problems. We do, however, monitor certain calls to our staff for quality purposes. If you object to this, you may come to one of our offices and speak with a customer service representative. In providing telephone services,

we do receive usage information, including numbers called and received and duration of calls. We retain this information, as long as required by some authorities or for billing purposes and treat all such information as private.

USE AND SHARING

Use Policy – We consider your information confidential, and use it only in providing our voice, video, broadband, and internet services for such things as sales, installation, operations, administration, advertising, marketing, support, network management, maintenance, customer care, communications with you, billing and collection, and for accounting and tax purposes. We may also use such information, in dealing with fraud and unauthorized use of our services, or when required under the law.

We use aggregate information about our customers and their usage for a variety of purposes. Such aggregated information does not identify individual customers. We may share such aggregate information with third parties in order to better offer product and service preferences to you but we will not share your own information with aggregate information or with information from others.

Sharing Policy – It is our policy not to disclose any personal identification information about you to others outside of Zirrus and our affiliates, vendors and business partners without your prior consent, except as permitted by law. We do not sell or provide your personal information to parties unrelated to the services we provide without your permission. As a further measure, you can affirmatively opt out of such sharing by writing to the return address on your billing statement, or you may contact us online at www.zirrus.com. You can also notify us in either way if you prefer not to receive certain types of marketing contacts from us.

Special Exceptions – We reserve the right to disclose your information if we have a good faith belief that it is necessary to: (1) comply with the law or legal process served on us; (2) protect and defend our rights or property or those of others; (3) respond to fraud, abuse or unauthorized reception; (4) enforce our Acceptable Use Policy or related standards; (5) act in an emergency to protect your safety or that of another. We may also share or transfer your information along with your account as a part of any sale or transfer of all or a portion of our business operations, merger or combination with another organization. In such a case, you will be notified of any changes in policy.

Outside Parties – Zirrus sometimes uses affiliates, vendors or partners in providing our services and may provide your information for such purposes. We require that outside parties maintain at least the same level of confidentiality that we maintain. In addition, any use by the vendor may not exceed that needed to provide its service. We do not share your information with other third parties without your consent. If you become a customer of a third party directly, you should review its privacy policy, as it may differ from ours.

Retention Policy – Zirrus may retain personal customer information in its regular business records as long as you are a customer or until no longer needed for business, tax or legal purposes. Our security measures for this information are discussed below.

Voice Services – Federal and some state regulations limit our use and sharing of certain information concerning a customer's telephone services. This information is known as "Customer Proprietary Network Information" or "CPNI", and includes information on how you use our telephone services, such as your call patterns, service features, price plans, spending profiles, call destinations and related information. In offering our spectrum of local and long distance telephone, we do use your telephone service information to offer new services and pricing plans. If you do not want us to use your CPNI for this purpose, you may contact us at (336) 463-5022 or you may contact us at www.zirrus.com. On the other hand, if you would like us to offer you information on video and data services or would like to learn more about our bundled offers, please contact us in any of the same ways. Consenting to allow us to use your CPNI will help us offer you the best and most up-to-date services. Your consent will remain in effect until you notify us you want to revoke or change your permission, or as limited by law.

Your choice will not affect the services you now receive. We do not disclose this information to unrelated parties, except as required by law.

Directory Listing – We offer our telephone customers the ability to designate their listings as non-published within print or electronic directories or directory assistance services. Because of the complexity of this process and the involvement of other entities in publishing, errors may occur from time-to-time. These and certain other telephone services are offered subject to tariff or contractual terms that limit our liability in the event of such errors.

Internet Services – We do not read your email messages, instant messages, online chats, or the content of other online communications that reside on or pass through our Service. We may however, retain and provide such communications if we are legally required to do so. Incoming and outgoing email messages are generally scanned automatically to identify and filter out likely spam or harmful messages and for viruses, spyware and related problems that could harm your equipment, the network or other users.

INTERNET SECURITY

Taking Proper Precautions – Maintaining the security of your personal computer is an important part of protecting your own privacy and of helping us protect our network and customers' service. You should follow our Authorized Use Policy. In order to prevent unauthorized access to your computer, you should regularly update all the software packages installed on your computer (including your antivirus, intrusion prevention, and operating system software) and uninstall software packages you do not use. You should also regularly perform antivirus scans with a reputable antivirus product and ensure any hardware-based security products are update and maintained based on the manufacturer's recommendations.

Persons with questionable intent may use the Internet or email to pose as someone you trust or do business with. You should always be sure who you are dealing with before clicking on an Internet link or giving personal information. To avoid all these and other forms of attack, we encourage you to visit our website at www.zirrus.com or the Federal Trade Commission ("FTC") at www.ftc.gov for regular updates and tips on protecting yourself. The management of Zirrus may take protective action related to your service or contact you directly with information from time-to-time to help with this effort. While we take reasonable steps to protect your services, we highly recommend that you regularly change your login password, using hard-to-guess combinations of numbers, letters, and special characters. Do not use words that are found in the dictionary as, or as a part of, your passwords. Once communications enter the Internet, it is possible for them to be accessed by third parties over whom we have no control. Moreover, since we cannot control the websites or services operated by third parties, you should review their terms of service and privacy policies and only visit website you trust.

Spam – Zirrus tries to prevent and block spam, and we encourage your help by preventing unauthorized access to your computer. We suggest that you remain up-to-date on ways to avoid and combat spam. We may use email to send transactional or relationship messages related to your service. If you prefer, you may opt-out of other marketing messages we may send by notifying us in response to any you may receive.

Cookies – A third party ad server that places ads on our websites may use "cookies" to collect anonymous information concerning your preferences. A "cookie" is a computer code added to a file on your computer as a record of its visit. It does not collect or provide your name or any other personal information about you. It can, however, be read by the website that placed it to note information about your visit, such as your type of web browser, operating system and Internet Protocol ("IP") address. It can also be used to recognize you when you log in as a registered user or as a repeat visitor returning to our website. This allows us to tailor our site by remembering you and any options you select. You can control what cookies are accepted by your computer through the settings on your web browser or by deleting them from your files. Doing so, however, may limit any personalization available to you.

Third-Party Cookies and Web Beacons – These forms of computer code are sometimes placed by advertisers or others with connection to a webpage and may be read by the ad's provider. They may use a form or code called a "web beacon" or "clear GIF." These are usually a transparent image on a webpage or email message and serve as a way to gather information about your visit such as your IP address as well as other information or statistics about your visit. As with cookies, you can use your browser settings to control web beacons with vendors, advertisers and others.

LAW ENFORCEMENT & LEGAL REQUESTS

Information Disclosure – We regularly receive legal requests from government and law enforcement personnel for customer information. We also receive discovery requests in civil litigation. In all such cases, we operate by providing such information as the law requires. The laws concerning your privacy and government access change from time to time and may affect how we are required to respond. Under current law, many criminal subpoenas require that we not disclose or notify you of the request. Due to this fact and the volume of requests we receive, we do not assume any duty to notify you of receipt of any legal requests.

Internet Information – Your account records and information concerning your Internet access may be subpoenaed by a governmental agency or by others through the courts. Internet messages and files shared over "peer-to-peer" services often include your IP Address, and you can be identified in this way if we receive a lawful subpoena. As with telephone interception, details concerning your Internet access and the content of communications can be obtained by law enforcement through a court order or similar authority. In addition, the law permits us to disclose to law enforcement, voluntarily and without prior notice, customer information, including the contents of communications, if we reasonably believe that an emergency involving immediate danger of death or serious physical injury requires such disclosure without delay.

Telephone Information – Current law requires law enforcement to obtain a court order or other similar authority for a telephone wiretap or to use a pen register or trap and trace device to capture dialing information. Law enforcement can also subpoena account and call record information.

SECURITY OF INFORMATION

We are aware of the many recently publicized instances of customer information security breaches. We continuously work on maintaining and deploying novel ways to protect your information. For our most sensitive databases, we use employee education and multiple intrusion prevention technologies combined with strict physical and logical access controls and strong encryption technologies with dedicated security staff to ensure security policy compliance. All of our third parties are periodically checked for security compliance. Nevertheless, although we endeavor to ensure the confidentiality and integrity of our information systems, we cannot guarantee that our security measures will prevent unauthorized access.

CHILDREN'S PRIVACY

The websites provided by Zirrus are not directed at, or intended for use by, children under the age of 13. We do not knowingly allow anyone under 18 to provide any personal information on our websites. Children should always get permission from a parent or guardian before sending personal information over the Internet. If you believe your child may have provided us with personal information, you can contact us at the address found on your monthly bill and we will delete this information. You can find more information about protecting children's privacy by contacting the FTC or viewing its website at www.ftc.gov.

CHILD PORNOGRAPHY

As a provider of an electronic communications service, we are required by law to report any evidence we may become aware of relating to violations of laws concerning child pornography.

CUSTOMER ACCESS TO INFORMATION

You may check the accuracy of personal information in your account by contacting a Customer Service representative. We also make a more complete review of your personally identifiable information available to you within a reasonable time following a request. You may examine the information and advise us of any errors you believe we should correct, upon prior request and at your own cost, during business hours at the Zirrus office listed on your billing statement.

YOUR ENFORCEMENT RIGHTS

You can enforce your legal privacy rights concerning our collection, use and sharing of your personally identifiable information.

OTHER TERMS AND CHANGES IN POLICY

Other terms and conditions affect our service offerings, including our Authorized Use Policy For High Speed Internet service, Tariffs and the Terms of Use for our websites. Changes in our service offerings, the law and policy may cause us to make changes to this and other policies from time to time. Any changes will be posted with the Online Privacy Policy at www.zirrus.com, which also contains provisions concerning privacy as relates to our websites.

ANNUAL DO-NOT-CALL REGISTRY NOTICE

In an effort to reduce the number of unwanted telemarketing calls, the FCC has provided telephone subscribers the opportunity to register their residential telephone numbers, including wireless numbers, for inclusion in the national Do Not Call (DNC) registry administered by the FTC. You may register, or revoke registration of, your number without charge by calling the FTC's toll free number, 1-888-382-1222 or TYY 1-866-290-4236, from the telephone number you are registering or revoking, or via online by visiting the FTC's website located at www.donotcall.gov. The FCC/FTC rules contain an "established business relationship" exception that permits a company that has such a relationship with you, like Zirrus, to call you even if your number is on this national DNC list. For more information, see <http://www.fcc.gov/cgb/donotcall/> and www.ftc.gov/bcp/conline/edcams/donotcall/index.html.