Privacy Policy

Carr Communications (hereinafter "Carr," "our," "us," or "we") is committed to respecting and protecting the privacy of our customers. Protecting your private information or Personally Identifiable Information is our priority. This Privacy Policy explains the types of personal information we collect, and how we collect, use, maintain, protect, and share this information. This Privacy Policy also tells you about the rights and choices you may have when it comes to your personal information.

This Privacy Policy applies to the information we collect when you use or interact with our products, services, and networks ("Services"), including https://site.carrinter.net/ ("Website"), but it is not exclusive to it. This Privacy Policy applies to everyone, including, but not limited to, visitors, users, and others who wish to access our Services or Website. By using our Services or Website, you consent to the data practices described in this Privacy Policy.

Please read this Privacy Policy carefully to understand our policies and practices regarding your information.

Definitions

- **Personal Identifiable Information or "personal information"** refers to any information that can be used to identify a specific individual. This includes information that is directly linked to a person, such as their name, date of birth, social security number, or email address, as well as information that can be used to identify them indirectly, such as their physical characteristics, biometric data, or online identifiers like IP addresses or device identifiers.

- **Allowable Tracked Information** refers to the specific types of data that a website or application is permitted to collect, use, and share with third parties. Examples of allowable tracked information that a website or application may collect and use could include: User behavior data, such as website usage patterns, search history, or clickstream data; location data, such as GPS data or IP address; demographic information, such as age, gender, or occupation; contact information, such as email address or phone number; or financial information, such as credit card numbers or payment information.

- **Third Party** refers to any entity that is not directly affiliated with us or our Website that is collecting or processing user data. This can include companies that provide services or products to us, analytics providers, or other third-party service providers. Examples of third parties that may be involved in the collection and processing of user data include: Analytics providers that collect data on user behavior and provide insights to the organization, or payment processors or financial institutions that process transactions and collect payment information, etc.

- **Cookies** refer to text files placed on a computer, mobile phone, or other device used to navigate the internet. Cookies transmit information back to the website's server about the

browsing activities of the user and may also be used to collect and store information about your preferences after you visit a website.

Information We Collect

We may collect information from you through communications such as the web, phone, email, or mail delivery, or through the services provided to you as the customer.

You may visit our Website without divulging any personal information; however, there are areas of the Website that might require personal information to contact us directly, specifically when registering emails, obtaining remote access, and contacting online technical support.

Information may also be collected in the following ways:

1. Browsing Our Website

IP addresses may be collected for the purposes of system administration, to gather broad demographic information, and to monitor the level of activity on our Website. Our log tracking collects visitors' IP addresses to analyze trends, administer our Website, track visitor movement, and gather broad demographic information to help determine the type of information visitors are interested in seeing on our Website. This tracking only collects IP addresses and not personally identifiable information. Visitors are not personally identifiable within our log files. We only use this information for internal purposes and do not share this information with non-affiliated companies or institutions.

Information may be collected regarding the referring URL, which browser you used to come to our Website, the pages of our Website that you viewed during your visit, and any search terms entered on our Website. We collect data about visitors to our subscriber website using some automated means such as Google Analytics, and reserve the right to use other methods such as cookies, clear GIFs, and passive automatic electronic collection. We may work with third-party companies to engage in such collection.

Customers may send us emails on our Website. We may retain the information in any email that you send to us, such as your name, email, address, or telephone number.

2. Broadband Internet Service

We may monitor the network and measure network performance and the performance of your Internet connection to improve our or the customer's overall service levels.

During communications with us for service support, we may also access information about your customer-premise equipment, such as computers, wireless modem devices, or other device settings, to provide customized technical support or to install specific applications or services for your use.

We reserve the right to access broadband traffic from individual accounts for the purposes of general network maintenance and management and upon request by law enforcement officials.

3. Provision of Information by Third Parties

We may obtain credit information about you from third parties when you purchase products or services from us.

How We Use the Information We Collect

We obtain and use customer information to provide you with quality telecommunications services. In addition to supporting the direct provision of service, this information may be used to protect customers, employees, and company property against fraud, theft, or abuse; conduct industry or consumer surveys; and maintain good customer relations. Access to databases containing customer information is limited to employees who need that information to perform their jobs. These employees are required to follow strict rules when handling customer information and are subject to disciplinary action if they fail to do so.

To better serve our customers, we may ask you questions to elicit additional information about your special needs and interests. For example, we may ask whether you work at home, whether any members of the household have special needs, or if teenagers reside in the household, to determine whether you may be interested in or benefit from additional lines or services. In all cases, the information we gather is used to facilitate the provision of quality customer service. We do not share this information with third parties to market non-Carr services to our customers.

We use information about customers in defined and responsible ways to manage, provide, and improve our products, services, and operations for our customers. This information will be used for internal purposes only and will not be shared with any third party. It shall not be used for any improper or unlawful purpose.

We retain customer information for such periods of time as required by law or regulation or as reasonably necessary to provide services.

E-mail Communications

From time to time, we may contact you via email for the purpose of providing announcements, promotional offers, alerts, confirmations, surveys, and/or other general communication. To improve our services, we may receive a notification when you open an email from us or click on a link therein.

If you would like to stop receiving marketing or promotional communications via email from us, you may opt out of such communications by clicking the “Unsubscribe” button at the bottom of the email.

If you choose to correspond with us through email, we may retain the content of your email messages along with your email address and our responses. We also may send automated messages to you pertaining to your account, such as billing invoices and other notices. We provide the same protections for these electronic communications that we employ in the maintenance of information received by mail or telephone. We ask that you not provide us with confidential information such as social security or account numbers through unsecured email. You may also contact us by phone, U.S. mail, or by visiting our location.

Use of Cookies

The Website may use "cookies" to personalize your online experience. Cookies are small pieces of data that are stored by a user's web browser on the user's hard drive. One of the primary purposes of cookies is to save you time. The purpose of a cookie is to tell the web server that you have returned to a specific page. For example, if you personalize website pages or register with our Website or services, a cookie helps us to recall your specific information on subsequent visits. This simplifies the process of recording your personal information, such as billing addresses, shipping addresses, etc. When you return to the same website, you can easily retrieve the information you previously provided.

You have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser settings to decline cookies if you prefer. If you choose to decline cookies, you may not be able to fully experience the interactive features of our services or our Website.

Links

This Website may contain links to other sites. Please be aware that we are not responsible for the content or privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read the privacy statements of any other site that collects Personally Identifiable Information.

Aggregate or Generic Information

This Privacy Policy does not apply to aggregate and/or generic information that does not identify you or any individual. Therefore, we reserve the right to share non-personal information with third parties for any reason, unless prohibited by law or regulation.

Managing Your Personal Information

We are committed to providing customers with opportunities to control how we use customer information about them. For example, customers may inform us of which telephone listings they want to include in our directories and in directory assistance and may also choose to have a non-published number, a non-listed number, or to exclude your address from your listing. Customers in areas where Caller ID services are available have the ability to block the display of their phone numbers and names. (Note that Caller ID blocking does not prevent the transmission of your phone number when you dial certain business numbers, including 911, or 800, 888, 877, and 900 numbers.) Further, customers can express a preference not to be called for marketing purposes (please see below, for more information on our "Do Not Call" policy). Customers may also opt out of our direct mailings and other service marketing programs. (Please see below, for our policy on the use of "Customer Proprietary Network Information"). A customer may indicate a change in such preferences at any time by contacting our customer service.

We do use individual customer information internally for planning purposes – so that we can, for example, develop, test and market new products and services that meet the needs of our

customers. Ordinarily, 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.

Sharing Information with Third Parties

Ordinarily, we will only share individual customer information with persons or entities outside the company to assist us in providing the services to which the customer subscribes as required by law or to protect the safety of customers, employees, or property.

We do not use third-party marketers, nor do we share access to individual customer information derived from the provision of our telecommunications services with other companies interested in marketing other services to our customers—and we would not do so without the customer's consent. We are committed to ensuring that customer information is not used without the knowledge and permission of our customers.

However, there are exceptions to our general practice. For example, unless you request otherwise, we may share certain personal or non-personal information with our affiliated companies with whom we have established business relationships. In addition, if we enter into a merger, acquisition, or sale of all or a portion of our assets, a customer’s personally identifiable information will, in most instances, be transferred as a part of the transaction, subject to required notices to affected customers.

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 our billed products and services. We are also required by law to provide billing name and address information to a customer’s long-distance carrier and other telephone companies to allow them to bill for telecommunications services. (By law, customers with non-published or unlisted services have the right not to have their billing name and address disclosed when they make a calling card call or accept a collect or third-party call. However, if they do restrict disclosure, they will be unable to make calling card calls or accept collect and third-party calls.)

Similarly, we are required to provide directory publishers with subscriber listing information—name, address, phone number, and, for yellow page advertisers, primary advertising classification—for the purposes of publishing and delivering directories. In addition, under certain circumstances, we may share customer information with other carriers or with law enforcement, for example, to prevent and investigate fraud or other unlawful use of communications services.

We may release customer information in response to requests from governmental agencies, including law enforcement and national security agencies, in accordance with federal statutory requirements or pursuant to court order. Before releasing any customer information, we will ensure that the underlying governmental request satisfies all procedural and substantive legal requirements and is otherwise proper. For example, we will ensure that any court orders are

valid, properly issued, and legally enforceable. Except as required by law or with the approval of the customer, we will not release any customer information in response to subpoenas or similar requests issued by private parties. Further, we will be diligent in authenticating the validity of any "governmental" request to ensure that the request actually originates from an authorized government agency.

Information Security

We take reasonable precautions to protect your personal information against unauthorized access. We require our personnel to be aware of and protect the privacy of all forms of customer communications and individual customer records.

We make it clear that employees who fail to comply with our privacy policies will face disciplinary action, which can include dismissal. All employees are trained regarding their responsibilities to safeguard customer privacy. We strive to ensure that the 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, and internal auditing techniques to protect against unauthorized use of terminals and entry into our data systems. We require that records be safeguarded from loss, theft, unauthorized disclosure, and accidental destruction.

In addition, sensitive, confidential, or proprietary records are 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 are 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, missing records and suspicious incidents involving records are referred to our Management. We encourage our employees to be proactive in implementing and enforcing our privacy policies. If employees become aware of practices that raise privacy or security concerns, they are required to report them to their supervisors.

Our regulatory department is responsible for ensuring that all our business units and their employees comply with privacy laws and regulations. We also require any consultants, suppliers, and contractors that may come into contact with customer proprietary information to observe these privacy rules with respect to any of our customers' individual customer information. They must abide by these principles when conducting work for us, and they will be held accountable for their actions.

While we have made significant efforts to protect your personal information, we cannot ensure or warrant the security of any information you transmit to us, and you do so at your own risk. Unfortunately, no data transmission over the Internet can be guaranteed to be 100% secure, and we will not be held liable should a third party illegally obtain your personal information via Internet transmission.

Children's Privacy

We do not provide services to children, and our Website is not targeted or marketed to children. We respect the privacy of your children, and we comply with the practices established under the Children's Online Privacy Protection Act. We do not knowingly collect or retain personally identifiable information from children. If you believe that a child has provided their information to us through our Website or Services, please contact us at 231-898-2244 so that we can take steps to delete it.

CPNI Notice

We want you to understand your rights to restrict the use of, disclosure of, and access to your Customer Proprietary Network Information, or CPNI. You have a right, and we have a duty, under federal law, to protect the confidentiality of your Customer Proprietary Network Information.

1. Definition of "Customer Proprietary Network Information."

The term "customer proprietary network information" is defined by federal statute to mean: (i) 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 relationship; and (ii) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

Examples of CPNI would be the telephone numbers that you call, the times you call them, the duration of your calls or the amount of your bill. Certain information relating to your use of our broadband Internet access services will also be considered CPNI and subject to additional privacy protections and use restrictions, including your broadband service plans, geographic location information, MAC and IP addresses, domain name information, device identifiers, traffic statistics, port information, application headers, usage and payload, as well as certain information pertaining to customer premises equipment and other customer device information, including consumer devices capable of connection to broadband services, such as smartphones, tablets, computers, modems and routers.

2. Use of Customer Proprietary Network Information.

Under federal law, you have the right to, and we have the duty to protect, the confidentiality of your CPNI. However, we may use CPNI without your consent, in a manner consistent with applicable law, to (i) initiate, render, bill, and collect for our services; (ii) market services among the categories of service to which you already subscribe; (iii) provide inside wiring installation,

maintenance, and repair services; (iv) provide maintenance and technical support for our services; (v) protect our rights and property, and protect users of our services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, these services; and (vi) provide any inbound telemarketing, referral, or administrative services for the duration of a customer-initiated call.

Further, after providing you with the required notice and opportunity to "opt-out," we may use your CPNI in a manner consistent with applicable law to market additional communications-related services to you and conduct surveys to improve our service offerings.

We will not use your CPNI for purposes other than those described above unless we first obtain your express "opt-in" consent. For example, without such consent, we will not use CPNI to market services not provided by us and will not share your CPNI with third parties (subject to the limitations discussed below).

3. Limits on the disclosure of CPNI outside of us.

As a general rule, we do not use third-party marketers and will not disclose your CPNI to third-party contractors without your explicit "opt-in" consent. This means that our records of the services you buy and the calls you make generally will remain private if you choose to keep them so, since we will not ordinarily disclose this information to outside parties without your permission. However, we will release customer information without involving you if disclosure is required by law or necessary to protect the safety of customers, employees, or property. For example: When you dial 911, information about your location may be transmitted automatically to a public safety agency.

Certain information about your long-distance calls may be transmitted to your long-distance company for billing purposes. We are also required by law to give competitive local exchange carriers access to customer databases to serve their customers, exchange credit information with other carriers, and provide listings (other than certain non-published and non-listed information) to directory publishers.

We will disclose information as necessary to comply with law enforcement statutes, such as to comply with valid, properly issued, and legally enforceable subpoenas, warrants, and court orders.

We may, where permitted by law, share CPNI with third parties where necessary to provide the services to which you subscribe, to protect our rights or property, and to protect users of our services and other carriers from fraudulent, abusive, or unlawful use of services.

We may, where permitted by law, provide CPNI to third parties such as credit bureaus or sell receivables to collection agencies to obtain payment for our billed products and services.

4. Authentication to prevent unauthorized access to CPNI.

We are committed to ensuring that only properly authorized individuals are able to access CPNI for legitimate purposes. This includes ensuring that any request by a "customer" to access CPNI is valid and properly authenticated, in accordance with applicable law and industry best

practices. In general, our internal policies and procedures are designed to ensure that CPNI is not released to unauthorized individuals.

Further, if a "customer" calls us to access "call detail records" (which include the number called, the number from which a call was placed, and the time, location, or duration of any call), we will not release those records unless (i) during the call, the customer provides a pre-established password; (ii) the information is sent to the customer's address of record; or (iii) after the call, we call the customer's telephone number of record to provide the requested information. If a "customer" attempts to access CPNI through our website, we will only provide such access if the customer has first established a password and backup authentication mechanism for the relevant account in a manner that does not rely on readily available biographical or account information. If a "customer" attempts to access CPNI by visiting a retail location in person, we will only provide such access if the "customer" presents valid photo identification matching the name of the record on the account. (Note that different procedures may apply to certain business customers served by a dedicated account representative where the underlying service agreement addresses CPNI protection and authentication.) We also will notify you at your address of record if anyone changes the access authorization or authentication information associated with your account.

5. Notice of unauthorized access to CPNI.

As a company, we are vigilant in our efforts to protect your CPNI. However, should we become aware that your CPNI has been accessed without proper authority, we will take swift action to fully document and address such unauthorized access and provide appropriate notice. In particular, we will (i) notify law enforcement (including the United States Secret Service and the Federal Bureau of Investigation) within seven business days; and (ii) notify you and any other affected customers within seven business days thereafter, unless earlier notification is necessary to avoid immediate and irreparable harm, or we are instructed by law enforcement personnel to refrain from providing such notice.

"Do Not Call" List

Any of our customers can express a preference not to be called by us for marketing purposes, and we will respect such preference. A customer who does not wish to receive sales calls from us specifically may ask to be placed on our company-specific "Do Not Call" list. We will note the customer's request immediately, although it may take up to 30 days for the customer's telephone number to be removed from any active lists or sales programs that are currently underway.

Any customer can ask to be put on our "Do Not Call" list by contacting our customer service department. All customers should call 231-898-2244. The requesting customer should provide, at a minimum, the telephone number that is the subject of the request, although inclusion of the customer's name and address is also useful. If a customer is served by multiple telephone numbers, the customer should tell us all numbers that should be placed on the "Do Not Call" list.

A residential customer will remain on our "Do Not Call" list for five years, and a business customer will remain on our "Do Not Call" list for one year unless the customer asks to be

removed from the list by contacting our customer service department. If a customer's telephone number ever changes, the customer must give us updated information in order for the "Do Not Call" status to remain in effect.

Notwithstanding the fact that a customer's telephone number is on our "Do Not Call" list, we may still contact that customer with respect to surveys, billing, and other service-related matters. Further, the customer should understand that being on our "Do Not Call" list will not prevent calls from other companies unaffiliated with us.

Privacy Policy Changes

We reserve the right to change, modify, or update this Privacy Policy at any time without notice. In the event of any modification, we will post the changes in this Privacy Policy so that you will always know what information we are gathering and how we might use that information. However, if such changes are material, we will either announce the change on the home page of the site or take such other action as we deem appropriate under the circumstances. Accordingly, you should periodically visit this page to determine the current Privacy Policy to which you are bound.

Contact Information

If you have questions about this Privacy Policy or wish to contact us concerning personal information you provided through the use of our Website, please call us at 231-898-2244, or toll-free at 800-431-1213.

You may contact us via regular mail at:

Carr Communications
4325 S. Masten Road
Branch, MI 49402