



HEART of IOWA

502 Main Street, PO Box 130
Union, IA 50258

Phone: 641-486-2211
www.heartofiowa.coop

PRIVACY POLICY

This Privacy Statement describes how Heart of Iowa hereinafter the “Company” collects information from or about you, either as a customer, visitor to any Company website, when you order services from us, how we use the information we collect, and the choices customers have concerning the collection and use of such information. The goal of this Statement is to ensure that your experience is secure so that you may use our products and services with complete confidence.

Personal Information Collected. Company limits the information collected about you to what is needed for conducting business, including the offering of products and services that might be of interest to you. You may choose to provide “personally identifiable information” (PII) to Company in a number of ways either in person, telephonically or via our websites or mobile apps. Examples of how you may share PII with us include: ordering a service or equipment from us, sending us email, responding to Company surveys, entering Company-sponsored contests or sweepstakes, registering to receive news or public information or applying for a job. We may also obtain PII from third parties (for example, credit agencies) with your permission.

Examples of PII are:

- Name (including company name for business customers)
- Unlisted or restricted mailing address
- Unlisted or restricted telephone number
- Email address
- Credit card number or financial/bank account number or information, including routing numbers
- Passwords or personal identification codes (PINs)
- Date of birth
- Company contact information for business customers
- Information obtained by Company through customer referral programs

The following information is not PII:

- Mailing address, unless unlisted or restricted at your request
- Telephone number, unless unlisted or restricted at your request
- IP Address allowing you to use our internet service
- PII included in aggregate data compiled by Company

The Company may compile or aggregate PII from numerous customers or Web visitors or mobile app users to collect data about groups of customers or potential customers or categories of service. Company does not consider this “aggregate” information as PII because the aggregate information does not contain the PII of any individual customer, Web visitor, or mobile app user.

Use of Personally Identifiable Information. The Company uses PII to provide products and services to meet customers' needs, including new products or services. Company may share PII with any Company-affiliated company, and these companies are subject to the terms of this Statement

The Company retains PII only as long as is necessary for Company to comply with business, tax and legal requirements. This retention period could be the entire time you are our customer depending on the type of PII.

Company does not:

- Sell any customer data, whether it be defined as PII or otherwise, to third parties.
- Collect PII from you unless you provide it to us in person, telephonically or electronically by visiting our websites or using our mobile apps, including information you provide in order to use our services.
- Sell the names and addresses of Company Web visitors or mobile app users to unaffiliated suppliers, without your prior approval
- Allow third parties to change your service provider or otherwise access your account information, at your request, without complying with our security policies, including our customer privacy policy that protects your account from changes not authorized by you.
- Information about our customers and users, including PII, may be shared and transferred as part of any merger, acquisition, sale of company assets or transition of service to another provider. This also applies in the unlikely event of an insolvency, bankruptcy or receivership in which customer and user records would be transferred to another entity as a result of such a proceeding.

Customer Proprietary Network Information (CPNI). CPNI is information that relates to the quantity, technical configuration, type, destination, location and amount of use of the telecommunications services purchased by you from Company. CPNI is available to Company solely through its relationship with you and information contained in your bill for telecommunication services. CPNI does not include information that is typically classified as PII, such as your name or email address and does not include compiled or aggregated PII. U.S. federal law requires Company to protect the confidentiality of CPNI.

Unless you opt-out from the use of CPNI, Company may use CPNI to market service offerings to you to which you do not already subscribe. Customer may contact the Company to opt-out. Company may, without prior approval from you, use CPNI to provide or market service offerings to you, if the service offerings are within the same categories of service to which you already subscribe, regardless of your CPNI selection of CPNI.

If you order Company services from a Company dealer, Company's dealers are prohibited from accessing or using your CPNI unless you sign a consent form authorizing Company to release your CPNI to the dealers. Dealers are required by Company to take all necessary measures to protect the confidentiality of your CPNI. As part of the dealers' agreements with Company, dealers agree that, upon termination of your Company services, the dealers will promptly return all of your CPNI to Company and will not retain any CPNI in any form.

Value-Added Services. Because we appreciate the trust you have placed in us, we continually look for ways to enhance your customer experience. From time to time, we may notify you about a Company product or service using the information you have provided to us either in person, telephonically or electronically by visiting our websites or using our mobile apps, including information you provide to use our services. We strive to limit our offers to those we think you would benefit from and appreciate receiving.

The Company complies with all applicable laws and regulations regarding “Do Not Call” Lists. Generally, Company is allowed to contact its customers, even if the customers are registered with federal or state Do Not Call Lists, because of our relationship with you. Company will, of course, honor any request to remove your name from our telephone, mail or email solicitation lists and will delete your information from existing files within a reasonable time period. Customer may contact the Company to arrange for these notifications to be discontinued.

Information Disclosed to Third Parties. The Company does not sell PII of its customers. In limited circumstances, Company may provide PII to third parties:

- To assist us in developing, promoting, establishing, maintaining, and/or providing Company-related products and services to you, including joint marketing efforts or promotions, but PII may not be used by the third parties for any other purpose;
- To assist us in establishing accounts, billing, collecting payment (i.e., credit bureaus and collection agencies), enforcing the Terms and Conditions or the Acceptable Use Policy of our Company services where permitted by law, and protecting or enforcing our rights or property, or the services of our other customers, from fraudulent, abusive, or unlawful use by you of our services;
- To comply, when required by law, with court or administrative orders, civil or criminal subpoenas, warrants from law enforcement agencies, federal or state regulatory requirements, mandatory governmental audits, E911 reporting requirements, grand jury investigations, civil or criminal governmental investigations, or reporting required by the National Center for Missing and Exploited Children, designated by federal law as a reporting mechanism for child pornography; and
- To appropriate law enforcement, 911 centers, or emergency services when Company, in good faith, believes the disclosure is necessary to protect a person, Company property, or the public from an immediate threat of serious harm.

Data Collection Technologies. In addition to PII identified above, we, or our third-party partners, may collect non-personal information automatically when you enter Company websites or use Company mobile apps, such as domain name, browser, your computer operating system, information about the Web page from which you linked to the website, and time spent on different parts of our websites or mobile apps. We or our partners may use this information to evaluate and improve the websites and mobile apps, and may share the information with third parties on an aggregated basis to enhance our products and services offered. This on-line information is typically collected via cookies, web beacons (see below for definitions), and/or other data collection technologies. Like virtually all other websites that you visit, we use cookies to deliver Web content specific to your interests and to control access to your personal shopping

cart after your initial entry. The cookie permits the server to recall information from your previous shopping trip, should you decide to think about your purchase. A cookie is not used to access or otherwise compromise the data on your hard drive. With most browsers, you can choose to change your browser settings to disable cookies. Please be aware that cookies may be required to complete certain functions on Company websites and other websites you may link to from Company websites, including making purchases or payments on your account.

Security Measures. The Company wants you to use our services with confidence, and therefore we use a number of security techniques designed to protect your information from unauthorized access, including firewalls and access control procedures.

- Company has physical, electronic, contractual, and managerial security measures in place to protect against the loss, misuse and alteration of information under our control. For example, when you place an order on a Company Website, the information you submit is encrypted using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol.
- Company employees are bound by non-disclosure agreements that prevent them from disclosing any PII or CPNI. Further, Company guidelines state that Company employees must abide by all state and federal privacy and security laws and regulations in the performance of their job duties.
- Our policies also limit access to PII to only those employees, contractors, agents, or representatives that require the information to perform their jobs or assist Company with providing products and services to you.

Children. Children under the age of majority should consult with their parents or guardian before furnishing any data to us. Parents should consider using one of a number of available parental control tools that provide a child-friendly, online environment and can prevent children from disclosing PII without parental consent. If a child has provided personal information without the consent of a parent or guardian, that parent or guardian should contact the Company to request that the information be deleted from our records. More information about parental controls may be found on Company websites or by contacting a Company customer care representative.

Company does not knowingly collect PII from children under the age of 13 in connection with providing products and services, and it strives to comply with all provisions of the Children's Online Privacy Protection Act (COPPA). If Company inadvertently collects information from minors below the age of 13, the information will be treated as PII of the adult customer.

Website Links. Company is not responsible for the content or privacy policies of other non-Company websites or non-Company mobile apps. You should keep this in mind when accessing websites through links on Company websites or mobile apps, or through third party advertisements appearing on Company websites or mobile apps. Further, Company may advertise on other websites or mobile apps. The advertising companies placing our ads may use cookies or web beacons to track the effectiveness of our ads. The use of such technology is subject to the privacy policies of the advertising companies, and not this Statement.

Statement Updates. We may update this Privacy Statement at any time in connection with our constant efforts to improve our products and services. We strongly encourage you to periodically review this Statement. We reserve the right to expand our capabilities for information collection and use and change this Statement in this regard. If any change constitutes a material change to this Statement, we will post a notice on our websites in a prominent position. If Company decides to use PII in a manner that is materially different from what is contained herein, we will post the change on this page for 30 days before making the change.

Security Breaches. While our goal is to prevent any unauthorized disclosure of PII, the Company cannot guarantee that a disclosure will not occur. We will make reasonable efforts to contact you if we determine that a security breach has occurred and that there is a reasonable risk of identity theft or as otherwise required by law.

Contact Us. If you have questions, concerns, or complaints about this Statement or Company's privacy practices, please contact customer service at:

Heart of Iowa
502 Main Street
PO Box 130
Union, IA 50258-0130
Email: customerservice@heartofiowa.coop
Phone: 1-800-806-4482 or 641-486-2211

We will respond to your inquiries in a timely manner.

Definitions Applicable to Privacy Policies. Cookies are small, encrypted data strings our server writes to your hard drive that contains your unique Company User ID. Web beacons are small graphic images imbedded in a webpage or email.

Internet Information. Company's network management practices are designed to provide the best possible online experience to its customers. To that end, Company monitors traffic flows between points within its network and between its network and locations on the Internet for purposes of reasonable network management. Company uses this information to manage its network, provide security for its customers, plan for future needs, and ensure its network runs efficiently. Monitored information includes the amount of data sent to and from your connection, the source and destination of the data, and the type of information sent and received. In limited circumstances, Company may also look into the contents of the information to determine whether it is malicious in nature (such as a virus, spam, abuse, copyright, worm, etc.) or when required by law to comply with judicial orders or regulations.

Updated November 20, 2025