

PRIVACY POLICY



Effective Date: October 1, 2026

OUR COMMITMENT TO YOUR PRIVACY

Allband Communications Cooperative and its affiliates (“Allband,” “we,” “us,” or “our”) respect the privacy of our customers and are committed to protecting personal information entrusted to us.

This Privacy Policy explains the types of information we may collect, how we use and disclose that information, how we protect it, and the choices and rights that may be available to you.

This Policy applies to information collected in connection with Allband’s telecommunications, broadband Internet, voice, and other communications services; customer accounts; websites; online services; customer support; billing; and related interactions with Allband (collectively, the “Services”).

Certain information associated with telecommunications services may also be protected as Customer Proprietary Network Information (“CPNI”) under federal law. Special protections applicable to CPNI are described below.

This Policy does not replace any rights or obligations established by applicable law, tariff, service agreement, or other Allband policy.

1. INFORMATION WE COLLECT

The information Allband collects depends on how you interact with us and the Services you receive.

We may collect the following categories of information.

Account and Contact Information

This may include:

- name;
- service and mailing address;
- email address;
- telephone number;
- account number;
- authorized users;
- account credentials;
- communication preferences; and
- other information necessary to establish and manage your account.

PRIVACY POLICY



Billing and Transaction Information

This may include:

- services and service plans purchased;
- charges, payments, and account balances;
- billing history;
- payment-related information;
- credit or collection information when applicable; and
- records concerning installation, repair, equipment, and other transactions.

Payment card, banking, or other payment information may be processed by Allband or by payment-processing providers acting on our behalf. Allband may limit the payment information it stores directly when a third-party payment provider processes a transaction.

Service and Network Information

When providing telecommunications or broadband services, Allband may collect information necessary to provision, operate, maintain, secure, troubleshoot, and improve those services.

Depending on the Service, this may include:

- service type and configuration;
- assigned network addresses;
- device and equipment information;
- connection and session information;
- network performance information;
- bandwidth and data-usage information;
- network event and diagnostic information;
- security-related logs;
- service availability and outage information; and
- other technical information generated through use of our network.

Allband does not routinely inspect the content of customer communications for advertising purposes. Technical information may, however, be analyzed or processed when reasonably necessary to operate, secure, troubleshoot, or protect the network or to comply with applicable law.

Customer Proprietary Network Information

For telecommunications services subject to federal CPNI requirements, Allband may possess Customer Proprietary Network Information.

CPNI generally includes information made available to a telecommunications carrier by virtue of the carrier-customer relationship that relates to the quantity, technical configuration, type,

PRIVACY POLICY



destination, location, or amount of use of telecommunications services, as well as certain information appearing on telecommunications bills.

Examples may include:

- telephone services purchased;
- features associated with a telephone line;
- call-detail information;
- calling patterns;
- service configuration;
- usage information; and
- certain billing information.

CPNI does not generally include subscriber-list information when that information is treated separately under applicable law.

Customer Support and Communications

When you contact Allband, we may collect:

- correspondence with you;
- customer service requests;
- technical support information;
- trouble-ticket information;
- records of account changes;
- feedback;
- complaints; and
- other information you voluntarily provide.

Calls or other communications with Allband may be recorded or monitored for training, quality assurance, security, documentation, dispute resolution, or other legitimate business purposes when permitted by law. Where notice or consent is required, Allband will provide it as required by applicable law.

Website and Online Information

When you visit an Allband website or use an Allband online service, certain information may be collected automatically.

Depending upon the technologies in use, this information may include:

- IP address;
- browser type;
- device type;
- operating system;

PRIVACY POLICY



- pages visited;
- referring website or source;
- date and time of access;
- website interaction information; and
- similar technical information.

Allband websites and services may use cookies, local storage, pixels, log files, analytics technologies, or similar tools when reasonably necessary to:

- provide website functionality;
- maintain sessions;
- remember preferences;
- protect security;
- prevent fraud;
- understand website performance;
- diagnose technical problems;
- measure usage; or
- improve online services.

Some third-party services integrated into Allband websites may also use their own cookies or similar technologies subject to their privacy practices.

Where required by applicable law, Allband will provide appropriate notice or choices concerning these technologies.

Information From Other Sources

We may receive information from third parties when appropriate to provide or protect our Services, including:

- payment processors;
- credit reporting agencies;
- collection agencies;
- contractors and service providers;
- telecommunications carriers;
- equipment vendors;
- software and cloud-service providers;
- cybersecurity providers;
- governmental entities;
- public records; and
- fraud-prevention or identity-verification providers.

2. HOW WE USE INFORMATION

Allband may use personal information for legitimate business, operational, security, and legal purposes, including to:

- establish and maintain customer accounts;
- provision and provide Services;
- authenticate customers and authorized users;
- install, maintain, repair, and troubleshoot Services and equipment;
- bill and collect payment;
- process transactions;
- communicate about accounts and Services;
- provide customer and technical support;
- respond to inquiries and complaints;
- detect and prevent fraud, identity theft, spam, malware, cyberattacks, and other abuse;
- protect customers, employees, facilities, equipment, and networks;
- manage network performance, reliability, capacity, and security;
- investigate violations of our agreements and policies;
- comply with legal and regulatory obligations;
- maintain records required for business or legal purposes;
- improve our Services, operations, and customer experience;
- develop and plan new services and network improvements;
- communicate about products or services when permitted by law; and
- exercise or defend Allband's legal rights.

We may also use aggregated or de-identified information for network planning, analytics, service improvement, research, reporting, or other legitimate purposes when the information does not reasonably identify an individual customer.

3. CUSTOMER PROPRIETARY NETWORK INFORMATION

Federal law provides special protections for Customer Proprietary Network Information.

Allband takes reasonable measures designed to protect CPNI against unauthorized access, use, or disclosure and maintains procedures designed to comply with applicable Federal Communications Commission requirements.

Allband may use or disclose CPNI without additional customer approval when permitted by law, including when necessary to:

- provide the telecommunications service from which the information is derived;
- provide services necessary to or used in the provision of that telecommunications service;
- initiate, render, bill, or collect for telecommunications services;
- provide customer-premises or inside-wiring installation, maintenance, or repair when permitted;

PRIVACY POLICY



- protect Allband's rights or property;
- protect customers or other carriers from fraudulent, abusive, or unlawful use;
- provide emergency services;
- respond to lawful governmental or legal requests; or
- perform other activities authorized by applicable law.

Where customer approval is required before Allband may use or disclose CPNI, Allband will obtain the level of customer approval required by applicable law.

Allband does not sell CPNI to third parties for their independent marketing purposes.

4. CPNI ACCOUNT SECURITY

Allband takes reasonable measures to authenticate customers before providing access to protected CPNI.

Depending on how a customer contacts us, authentication measures may include:

- passwords or passcodes;
- online account credentials;
- verification through contact information already associated with the account;
- one-time verification codes;
- account-specific information;
- identity-verification procedures; or
- other methods permitted or required by law.

Allband may provide notifications concerning certain account changes, credential changes, or access to CPNI when required by applicable FCC rules.

Customers should protect their account credentials and promptly notify Allband if they believe their account or authentication information has been compromised.

5. EMERGENCY SERVICES AND LOCATION INFORMATION

When you use emergency calling services such as 911, information necessary to facilitate an emergency response may be transmitted to a public safety answering point, emergency service provider, governmental agency, or other entity involved in providing emergency assistance.

Depending on the Service and technology involved, this information may include:

- telephone number;
- registered service address;
- device location;
- callback information; or
- other information used to identify the caller or location.

6. WHEN WE DISCLOSE INFORMATION

Allband does not sell customers' personal information or CPNI to data brokers or third parties for their independent advertising or marketing purposes.

We may disclose personal information in the following circumstances.

Service Providers and Contractors

Allband may provide information to vendors, contractors, consultants, and other service providers that perform services on our behalf.

These may include providers supporting:

- billing;
- payment processing;
- customer communications;
- email or text messaging;
- customer-service platforms;
- accounting;
- information technology;
- network operations;
- equipment installation or repair;
- cloud or data-hosting services;
- cybersecurity;
- software platforms;
- professional services;
- mailing and printing;
- collections; and
- other operational functions.

Allband expects service providers that receive customer information to use that information only as necessary to provide services to Allband or as otherwise permitted by applicable law and contract, and to maintain reasonable safeguards appropriate to the information involved.

Other Telecommunications Providers

Information may be exchanged with other telecommunications carriers, network operators, interconnection partners, service providers, or vendors when reasonably necessary to:

- provision Services;
- route or complete communications;
- support customer services;
- troubleshoot technical issues;
- bill for Services;

PRIVACY POLICY



- prevent fraud or abuse; or
- maintain network security.

Credit and Collections

Where permitted by law, Allband may obtain information from or provide information to:

- credit reporting agencies;
- collection agencies;
- financial institutions;
- payment processors; or
- similar entities

for purposes such as evaluating credit, collecting amounts owed, processing payments, preventing fraud, or managing account risk.

Legal and Regulatory Requirements

Allband may disclose information when we reasonably believe disclosure is required or permitted by:

- applicable law;
- regulation;
- legal process;
- court order;
- subpoena;
- warrant;
- regulatory requirement; or
- lawful governmental request.

Protection of Allband and Others

Allband may disclose information when reasonably necessary to:

- detect or investigate fraud;
- prevent abuse or unlawful use of Services;
- protect network or information security;
- protect the safety of customers, employees, or members of the public;
- protect Allband's property, facilities, or legal rights;
- investigate violations of Allband agreements or policies; or
- respond to an emergency involving danger of death or serious physical injury when permitted by law.

Business Transactions

If Allband participates in a merger, acquisition, financing, restructuring, consolidation, transfer of assets, or similar business transaction, relevant information may be transferred or disclosed as permitted by law and subject to appropriate protections.

7. WE DO NOT SELL CUSTOMER INFORMATION FOR THIRD-PARTY ADVERTISING

Allband does not sell customer CPNI or personal information to third parties for those third parties to independently market unrelated products or services to Allband customers.

Allband also does not use broadband network traffic information to create individualized profiles for sale to third-party advertisers.

If Allband's practices materially change in the future, this Privacy Policy will be updated and any notice, approval, or consent required by applicable law will be provided before the new practice begins.

8. NETWORK MANAGEMENT AND SECURITY

Operating a reliable communications network requires Allband to collect and analyze certain technical and network information.

Allband may inspect, process, or analyze network traffic information, metadata, connection information, equipment status, diagnostic information, and security events when reasonably necessary to:

- operate the network;
- manage network capacity and performance;
- identify and resolve congestion;
- diagnose technical problems;
- identify outages;
- detect malicious traffic;
- prevent denial-of-service attacks;
- detect malware, botnets, spam, phishing, or other abuse;
- identify compromised customer equipment;
- investigate security incidents;
- protect customers and network infrastructure;
- comply with legal requirements; or
- enforce applicable service agreements and acceptable-use policies.

Allband does not represent that it continuously reviews the content of customer Internet communications.

PRIVACY POLICY



When technical inspection or processing is reasonably necessary for network operation, security, troubleshooting, fraud prevention, or legal compliance, Allband seeks to limit that activity to what is reasonably necessary for the relevant purpose.

Network-management activities are conducted consistent with applicable law and Allband's published network-management and broadband disclosures.

9. INFORMATION SECURITY

Allband maintains administrative, technical, and physical safeguards designed to protect personal information against unauthorized:

- access;
- acquisition;
- destruction;
- loss;
- misuse;
- alteration; or
- disclosure.

Security practices may include measures concerning:

- access controls;
- multifactor authentication where appropriate;
- account authentication;
- employee training;
- physical security;
- network security;
- logging and system monitoring;
- vulnerability management;
- security updates and patch management;
- encryption where appropriate;
- vendor management;
- incident response;
- data backup and recovery; and
- other safeguards appropriate to the nature of the information and systems involved.

Access to sensitive customer information should be limited to employees, contractors, and systems with an appropriate business or operational need.

No information system, network, transmission method, or storage system can be guaranteed to be completely secure. Allband therefore cannot guarantee that unauthorized access or a security incident will never occur.

10. DATA BREACH AND SECURITY INCIDENT RESPONSE

Allband maintains procedures for identifying, containing, investigating, and responding to suspected or confirmed security incidents involving customer information.

These procedures may include:

- containing affected systems;
- preserving relevant evidence;
- investigating the nature and scope of an incident;
- determining what information may have been affected;
- taking corrective measures;
- resetting or protecting account credentials when appropriate;
- coordinating with service providers or law enforcement when appropriate; and
- providing legally required notifications.

If Allband determines that a security incident requires notification to affected individuals, governmental agencies, law enforcement, regulators, or other parties, Allband will provide such notification in accordance with applicable federal and state requirements.

11. DATA RETENTION

Allband retains personal information only for as long as reasonably necessary for legitimate business, operational, security, contractual, or legal purposes.

Factors affecting retention periods may include the need to:

- provide Services;
- maintain customer accounts;
- maintain billing and payment records;
- meet accounting and tax requirements;
- resolve disputes;
- collect amounts owed;
- prevent fraud and abuse;
- investigate security incidents;
- maintain network security;
- satisfy regulatory recordkeeping requirements;
- respond to legal claims; and
- enforce applicable agreements.

Different categories of information may therefore be retained for different periods.

When information is no longer reasonably required, Allband may delete, destroy, anonymize, or de-identify it in accordance with applicable legal requirements and company procedures.

12. CHILDREN'S PRIVACY

Allband's general consumer Services and websites are not directed to children under 13.

Allband does not knowingly collect personal information directly from children under 13 through its general website or online Services in a manner subject to the Children's Online Privacy Protection Act ("COPPA") without the consent required by law.

If Allband learns that personal information from a child has been collected in circumstances requiring parental consent, Allband will take reasonable steps to delete or otherwise appropriately address the information.

Parents and guardians remain responsible for supervising minors' use of Internet and communications services made available through their household account.

Allband may require an adult subscriber or other legally authorized person to establish or modify an account.

13. DIRECTORY LISTINGS AND VOICE PRIVACY OPTIONS

For voice services where directory-listing services remain available, customers may have options concerning publication or disclosure of their telephone directory information.

Depending on the applicable service and directory provider, these options may include:

- listed service;
- non-listed service;
- non-published service; or
- restrictions on address information associated with a listing.

The availability, terminology, fees, and operation of these options may change depending on the voice service or directory provider.

Allband may also offer privacy-related calling features, such as caller identification or caller-ID blocking, where supported by the applicable service.

Customers should contact Allband for current information regarding available directory and voice privacy options.

14. EMAIL, TEXT MESSAGES, AND CUSTOMER COMMUNICATIONS

Allband may communicate with customers by mail, telephone, email, text message, online account message, or other methods concerning:

- account activity;

PRIVACY POLICY



- billing;
- payments;
- outages;
- planned maintenance;
- service changes;
- security matters;
- regulatory notices;
- customer support;
- installation or repair;
- service availability;
- community or cooperative matters; and
- products or services.

Some communications are necessary to administer the customer relationship or provide the Service and may not contain an unsubscribe option.

Where Allband sends promotional email or text communications subject to applicable marketing laws, recipients will be provided with any opt-out mechanism required by law.

15. COOKIES, ANALYTICS, AND SIMILAR TECHNOLOGIES

Allband does not make a blanket representation that its websites operate without cookies or other online technologies.

Allband websites, customer portals, payment tools, embedded applications, or third-party services may use cookies or similar technologies depending on the functionality being provided.

These technologies may support:

- website functionality;
- security;
- authentication;
- session management;
- customer portals;
- payment processing;
- preference storage;
- performance measurement;
- troubleshooting;
- analytics; and
- other legitimate website operations.

Third-party services integrated into Allband websites may independently use cookies or related technologies in accordance with their own privacy policies.

PRIVACY POLICY



Users may be able to control certain cookies through browser or device settings. Blocking or deleting cookies may cause some website functions to operate differently or become unavailable.

Allband will update its disclosures when its material website data practices change.

16. THIRD-PARTY WEBSITES AND SERVICES

Allband websites may contain links to websites, portals, applications, payment processors, social media services, or other resources operated by third parties.

A link from an Allband website does not mean that Allband controls or endorses the third party's privacy or security practices.

Information submitted directly to a third-party service is subject to that provider's own privacy policy and terms.

Customers should review the privacy practices of third-party services before providing information directly to them.

17. IDENTITY THEFT AND FRAUD PREVENTION

Allband maintains policies and procedures designed to identify, detect, prevent, and respond to identity theft, account takeover, payment fraud, and other suspicious activity when required or appropriate under applicable law.

These procedures may include:

- customer authentication;
- verification procedures;
- account monitoring;
- employee training;
- escalation procedures;
- fraud detection;
- credential protection; and
- other reasonable safeguards.

For security reasons, Allband does not publish detailed fraud-detection methods, internal thresholds, security configurations, or other information that could facilitate circumvention of those controls.

18. LAW ENFORCEMENT AND CALEA

Allband complies with the Communications Assistance for Law Enforcement Act ("CALEA") and other applicable laws governing lawful access to communications and call-identifying information.

PRIVACY POLICY



Allband provides access to communications or customer information to law enforcement or governmental authorities only when required or permitted by applicable law and pursuant to appropriate legal process or authorization.

Allband maintains internal procedures designed to ensure that legally authorized interception or access is implemented by appropriately authorized personnel and consistent with applicable FCC requirements and Allband security procedures.

Nothing in this Policy means that governmental authorities have unrestricted or routine access to Allband customer communications.

Allband may challenge, seek clarification of, or otherwise respond to legal demands as permitted by law.

19. CUSTOMER ACCESS AND CORRECTION

Customers may contact Allband to request assistance updating or correcting certain account information.

Before disclosing or modifying protected information, Allband may require reasonable authentication to verify the identity or authority of the person making the request.

Additional rights concerning personal information may apply under federal or state law depending on:

- the type of information involved;
- the Service involved;
- the customer's relationship with Allband; and
- applicable law.

Allband will respond to legally valid requests in accordance with applicable requirements.

20. PRIVACY CHOICES

Depending on the Services you use and applicable law, you may have choices concerning:

- marketing communications;
- directory publication;
- certain uses of CPNI;
- account communication preferences;
- optional text or email communications;
- cookies or similar technologies; and
- other optional uses of information.

Some uses of information are necessary to:

PRIVACY POLICY



- provide the Services;
- operate the network;
- secure accounts;
- process payments;
- troubleshoot problems;
- prevent fraud;
- comply with law; or
- maintain the customer relationship.

Those uses generally cannot be declined while retaining the applicable Service.

21. EMPLOYEE, CONTRACTOR, AND VENDOR CONFIDENTIALITY

Allband employees with access to customer information are expected to handle that information in accordance with:

- their job responsibilities;
- Allband policies;
- confidentiality requirements;
- security procedures; and
- applicable law.

Access to sensitive customer information should be limited to personnel who have an appropriate business or operational need.

Allband also relies on contractors and service providers to perform certain functions. Where appropriate, Allband uses contractual, technical, administrative, or other safeguards designed to require those parties to protect confidential customer information.

Allband may periodically review material service-provider relationships as part of its privacy, security, and vendor-management practices.

22. CHANGES TO THIS PRIVACY POLICY

Allband may update this Privacy Policy from time to time to reflect changes in:

- Services;
- technology;
- website functionality;
- vendors;
- business practices;
- security practices;
- legal requirements;
- regulatory requirements; or
- the ways Allband collects, uses, or discloses information.

PRIVACY POLICY



The current version will be posted on Allband's website with its effective date.

When required by applicable law, regulation, or agreement, Allband will provide additional notice of material changes or obtain customer consent.

Allband will not treat an update to this Policy as authorization for a materially different use of previously collected information when applicable law requires additional notice or consent.

Customers are encouraged to review this Policy periodically.

23. OTHER ALLBAND POLICIES AND TERMS

This Privacy Policy should be read together with Allband's applicable:

- Terms and Conditions;
- Acceptable Use Policy;
- Network Management Policy or disclosures;
- broadband consumer disclosures;
- tariffs;
- customer agreements;
- CPNI notices;
- service-specific terms; and
- other applicable notices.

This Privacy Policy describes Allband's information practices and does not create a separate limitation-of-liability regime.

Any contractual limitations of liability are governed by the applicable service agreement, tariff, Terms and Conditions, or other contractual documents.

Where applicable law or a service-specific requirement provides greater protection, Allband will follow the applicable requirement.

24. CONTACT US

Questions, comments, concerns, or requests regarding this Privacy Policy may be directed to:

Allband Communications Cooperative

7251 Cemetery Road
Curran, Michigan 48728

Phone: (989) 369-9999

Email: info@allband.org

Website: www.allband.org

PRIVACY POLICY



Customers who believe their account has been compromised or who become aware of a potential privacy or security concern involving Allband should contact Allband promptly.

Privacy Policy — Effective October 1, 2026