

## **BANTOR PRIVACY POLICY**

*Effective Date: May 4, 2026 | Last Updated: May 4, 2026*

This Privacy Policy explains how Muse Systems, Inc. ("Bantor," "we," "us," or "our") collects, uses, shares, and protects information in connection with the Bantor service available at bantor.ai and app.bantor.ai (the "Service"). It applies to information we process as a controller (for example, information about visitors to our website and our customers' Account administrators), and describes how we process information on behalf of our customers (for example, the audio, transcripts, and other content our customers choose to put into the Service).

Bantor is offered solely to users in the United States. We do not market the Service to, and do not knowingly permit use by, individuals or entities outside the United States. If you are located outside the United States, please do not use the Service.

### **1. Scope and How to Read This Policy**

Two roles, one policy. When you visit bantor.ai, sign up for an Account, or interact with our marketing or support, Bantor acts as a "business" or "controller" of your personal information. When our customers use the Service to record, transcribe, store, or analyze conversations, Bantor acts as a "service provider" or "processor" on those customers' behalf. The customer (typically the customer's employer) decides what content to put into the Service and is responsible for the lawful basis to do so. If you are a participant in a conversation that someone else recorded using Bantor, your relationship is primarily with that customer, and questions about that recording should be directed to them; you may also contact us at [privacy@bantor.ai](mailto:privacy@bantor.ai) and we will assist where we can.

### **2. Information We Collect**

#### **2.1 Information You Provide Directly**

- Account information: name, email address, password, job title, company name, phone number (where provided), and similar registration details.
- Billing information: payment card or bank-account details, billing address, and tax identifiers. We do not store full payment-card numbers; this information is collected and processed by our payment processor (Stripe).
- Communications: messages and feedback you send us, including support tickets, sales inquiries, and survey responses.
- Marketing preferences: opt-ins or opt-outs for newsletters, product updates, and event invitations.

#### **2.2 Customer Content**

Customer Content includes the audio, video, text, transcripts, summaries, notes, recordings, and other materials our customers and their Authorized Users submit to or generate through the Service. Customer Content may include the personal information of customers' employees and of third parties our customers communicate with. As to Customer Content, Bantor acts as a service provider or processor under our customers' direction, and our use is limited to what is necessary to operate the Service and to create Aggregated Data as described in Section 4, and we do not use Customer Content for any other purpose.

### **2.3 Information Collected Automatically**

- Usage data: pages and features viewed or used, clicks, session duration, error events, and similar telemetry.
- Device and connection data: IP address, browser type and version, operating system, device identifiers, and approximate location derived from IP address.
- Cookies and similar technologies: see Section 9.

### **2.4 Information from Third Parties**

- Single sign-on and integration partners: when you authenticate with a third-party identity provider (e.g., Google) or connect a third-party tool (e.g., a calendar or CRM), we receive the information you authorize that provider to share.
- Sales and marketing tools: we may obtain business contact data from publicly available sources or from data providers that represent the data has been collected lawfully.
- Service providers: we receive operational information from our subprocessors, such as transcription confidence scores, analytics, and error diagnostics.

## **3. Sensitive Information and Restricted Categories**

We do not request and ask that you do not provide certain categories of sensitive information through the Service, including: (a) protected health information subject to HIPAA, (b) full payment card numbers, (c) Social Security numbers or other government-issued identifiers, (d) information about children under thirteen (13), and (e) information collected in K–12 educational settings. Customers are responsible for ensuring that Customer Content does not contain these categories unless we have separately agreed in writing to support such use. See also Section 4.3 of the Terms of Service.

## **4. How We Use Information**

We use the information we collect to:

- provide, operate, secure, and support the Service, including transcription, summarization, scoring, and other AI-generated outputs the customer has requested;
- process payments and manage subscriptions;
- communicate with you about the Service, including service announcements, security alerts, billing notices, and (with consent where required) marketing messages;
- personalize and improve the Service, fix bugs, and develop new features;
- protect against fraud, abuse, and security incidents, and enforce our Terms of Service;
- comply with legal obligations, including responding to lawful requests from public authorities;
- produce aggregated, statistical, or de-identified data for any lawful business purpose, including analytics, benchmarks, research, marketing materials, and commercialization, licensing, or sale of such aggregated data, in each case in a manner that does not identify any individual or customer.

We implement reasonable technical and organizational measures designed to ensure that aggregated or de-identified data cannot reasonably be used to identify individuals or customers.

#### **4.1 No Training of General-Purpose AI Models on Identifiable Customer Content**

We do not use raw, identifiable Customer Content (including audio recordings, transcripts, or other identifiable inputs) to train, fine-tune, or otherwise improve general-purpose machine-learning models that we or our subprocessors operate. We may use aggregated and de-identified data derived from Customer Content to evaluate Service quality, build benchmarks, and improve features, in each case in a manner that does not identify customers, Authorized Users, or Third-Party participants.

### **5. Recording and Consent**

The Service enables our customers to record and transcribe conversations. Recording laws differ across U.S. states; some require consent of all parties, while others require consent of only one. Bantor does not, by default, play any audible disclosure or display any visual notice to participants. Bantor does not provide, enforce, or verify consent mechanisms and disclaims responsibility for customers' failure to obtain legally required consent. Our customers are solely responsible for providing required notices and obtaining required consents from every participant in a conversation. Bantor acts solely as a technology provider and does not determine the legality of any recording. Responsibility for compliance with applicable recording laws rests entirely with the customer. If you are a participant in a recorded conversation and have questions or concerns about that recording, please contact the customer that initiated the recording. You may also contact [privacy@bantor.ai](mailto:privacy@bantor.ai) for assistance.

## 6. How We Share Information

We share information in the following circumstances and not in any other way:

- With service providers (subprocessors): vendors that help us operate the Service under written contracts that limit their use of personal information to providing services to us.
- With customers: if you are an Authorized User, we share your activity, account, and Customer Content with the customer that owns your Account. Customer administrators can typically see usage analytics and Customer Content within their organization's Account.
- With your direction: when you authorize integrations with third-party tools (e.g., a calendar or CRM), we share information with those tools to fulfill the integration.
- For legal reasons: where required to comply with applicable law, regulation, legal process, or governmental request, or where we believe disclosure is necessary to protect rights, property, or safety.
- In a corporate transaction: if Bantor is involved in a merger, acquisition, financing, reorganization, or sale of assets, your information may be transferred subject to standard confidentiality protections.

We do not sell personal information for money. However, we may use, commercialize, or provide aggregated and de-identified data in a manner that does not identify any individual or customer. To the extent any of our analytics or advertising activities are deemed a "sale" or "share" under U.S. state privacy laws, you may opt out as described in Section 11.

## 7. Subprocessors

Bantor relies on a small number of third-party providers to operate the Service. Categories include cloud hosting, audio transcription, AI inference, telephony, email and messaging, error tracking, product analytics, and payment processing. A current list of our subprocessors is maintained at [bantor.ai/subprocessors](https://bantor.ai/subprocessors). Customers are notified of material changes to that list as described in their agreement with us.

## 8. Data Retention

We retain personal information for as long as necessary to provide the Service, comply with our legal obligations, resolve disputes, and enforce our agreements. The default retention practices are summarized below.

Category	Default retention
Account information	For the life of the Account, plus up to 90 days after termination for closeout and audit purposes.
Customer Content (audio, transcripts, summaries, notes)	For the life of the Account. After Account termination, Customer Content is available for export for 30 days, then deleted or de-identified within a commercially reasonable period.
Billing records	Up to 7 years to satisfy tax, accounting, and audit requirements.
Logs and security telemetry	Typically 30–365 days, depending on the system and security need.
Aggregated and de-identified data	Indefinitely; this data does not identify individuals.
Marketing contacts	Until you opt out, plus a brief suppression-list retention to honor your opt-out.

Where law requires longer retention, or where information is subject to a legal hold, we will retain the affected information for the additional period required.

## 9. Cookies and Similar Technologies

We use cookies, local storage, pixels, and similar technologies on [bantor.ai](https://bantor.ai) and [app.bantor.ai](https://app.bantor.ai). We use them for: (a) strictly necessary purposes (authentication, security, load balancing); (b) performance and analytics (understanding how the Service is used so we can improve it); and (c) where applicable, marketing and attribution. You can control cookies through your browser settings or, where offered in your jurisdiction, through an in-product preference center. Disabling strictly necessary cookies will impair the Service. We do not use cookies for cross-context behavioral advertising directed at children, and we honor recognized opt-out signals such as Global Privacy Control where required by law.

## 10. Security

We implement administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, alteration, disclosure, and destruction. Measures include encryption in transit and at rest for Customer Content, role-based access controls, logging and monitoring, vulnerability management, and personnel training. No service is perfectly secure, however, and we cannot guarantee the security of any information transmitted to or from the

Service. If you believe your Account has been compromised, contact us promptly at [legal@bantor.ai](mailto:legal@bantor.ai).

## 11. Your Privacy Rights (U.S. State Laws)

Depending on the U.S. state in which you reside, you may have the following rights with respect to personal information we process about you as a controller:

- Right to know: request the categories and specific pieces of personal information we have collected about you, the sources, the purposes for collection, and the categories of recipients.
- Right to delete: request deletion of personal information we have collected from you, subject to certain exceptions.
- Right to correct: request correction of inaccurate personal information.
- Right to portability: request a copy of your personal information in a portable format.
- Right to opt out of "sale" or "sharing": to the extent any disclosure of personal information for analytics or advertising purposes is considered a "sale" or "share" under your state's law, you may opt out.
- Right to limit use of sensitive personal information: where applicable, you may limit our use of certain sensitive categories.
- Right to non-discrimination: we will not discriminate against you for exercising any of these rights.

To exercise these rights, email [privacy@bantor.ai](mailto:privacy@bantor.ai). We will verify your identity by reasonable means before responding (for example, by confirming information associated with your Account). You may use an authorized agent to submit a request, subject to our verification of the agent's authority. We will respond within the time period required by applicable law (generally 45 days), and we may extend that period where permitted. We do not charge a fee for responding unless your request is manifestly unfounded or excessive.

If you are an Authorized User and your request relates to Customer Content, the customer that owns your Account is generally the controller, and we will route your request to that customer or assist you in contacting them.

## 12. California-Specific Disclosures

In addition to the rights described in Section 11, the California Consumer Privacy Act, as amended by the CPRA, requires us to disclose the following:

- Categories of personal information collected in the past 12 months: identifiers; commercial information; internet or electronic network activity; geolocation

(approximate); audio, electronic, or similar information (Customer Content); professional or employment information; and inferences drawn from the foregoing.

- Categories of sources: directly from you, automatically from your use of the Service, and from third parties as described in Section 2.
- Business or commercial purposes for collection: as described in Section 4.
- Categories of third parties to which information is disclosed: as described in Section 6.
- "Sale" or "sharing" of personal information: we do not sell personal information for money. Some analytics or marketing activity may be considered "sharing" under California law; you may opt out at [privacy@bantor.ai](mailto:privacy@bantor.ai).
- Sensitive personal information: we do not use or disclose sensitive personal information beyond the purposes permitted by California law.
- Retention: as described in Section 8.

If you are a California resident, you may also designate an authorized agent to submit a request on your behalf, subject to our verification.

### **13. Children**

The Service is not directed to and is not intended for individuals under eighteen (18) years of age. We do not knowingly collect personal information from children under thirteen (13). If you believe we have collected information from a child under thirteen, please contact [privacy@bantor.ai](mailto:privacy@bantor.ai) and we will take appropriate steps to delete it.

### **14. Geographic Scope**

The Service is offered solely in the United States. Bantor processes personal information in the United States. We do not market the Service to, and do not knowingly accept users from, the European Economic Area, the United Kingdom, or other jurisdictions outside the United States. If you access the Service from outside the United States, you do so at your own risk and consent to the transfer of your information to the United States.

### **15. Third-Party Sites and Integrations**

The Service may contain links to, or integrate with, third-party websites and services. This Privacy Policy does not apply to those third parties. We encourage you to review the privacy notices of any third-party site or service you interact with through the Service.

### **16. Changes to this Policy**

We may update this Privacy Policy from time to time. For material changes, we will provide at least thirty (30) days' advance notice by posting the updated policy at [bantor.ai/privacy](https://bantor.ai/privacy), sending an email to the address associated with Account administrators, and providing in-app notice. For non-material changes, we may post the updated policy without separate notice. The "Last Updated" date at the top of this policy reflects the most recent revision.

## **17. Contact Us**

Questions, requests, or complaints about this Privacy Policy or our processing of personal information? Contact us at:

**Email:** [privacy@bantor.ai](mailto:privacy@bantor.ai)

If you have not received a satisfactory response, you may also contact your state attorney general's office or relevant regulator.