

Accela, Inc.

Responsible AI Use Policy

How we use artificial intelligence — in our operations and across our products

A transparency statement for our customers and partners

Document Title	Responsible AI Use Policy
Audience	Customers, prospective customers, and partners
Classification	Public — may be shared externally
Version	1.1
Effective Date	August 20, 2026
Next Review	Reviewed at least annually
Policy Owner	Legal & Compliance / AI Governance Program
Related Documents	Privacy Policy (accela.com/privacy-policy); Accela AI Product Specific Terms (www.accela.com/terms/); your agreement with Accela, including any data processing terms

Contents

.....	1
1. Our Commitment to Responsible AI.....	1
2. Scope of This Policy.....	1
3. Our Responsible AI Principles.....	1
4. How We Use AI Internally.....	1
5. How AI Is Used in Our Products and Services.....	1
6. Your Data and AI.....	1
7. Human Oversight and Accountability.....	1
8. Third-Party AI Providers and Sub-Processors.....	1
9. Protections for Government and Regulated Customers.....	1
10. Security and Data Protection.....	1
11. Privacy and Your Rights.....	1
12. Governance and Continuous Oversight.....	1
13. Contact Us and Changes to This Policy.....	1
14. Key Terms.....	1

1. Our Commitment to Responsible AI

Artificial intelligence (AI) helps us deliver better, faster, and more reliable services to the organizations we serve. Accela uses AI thoughtfully to improve how we operate internally and to add value within our products. We do so under a formal governance program designed to protect your data, your rights, and the trust you place in us.

This policy explains, in plain language, how we use AI and the safeguards that govern that use. It is written for our customers and partners so that you can make informed decisions about working with us. We believe transparency is the foundation of responsible AI, and we commit to keeping this policy current as our practices and the regulatory landscape evolve.

Our core promises

We do not use your data to train third-party or publicly available (“foundation”) AI models.

A qualified person reviews AI-generated output before it is used to make decisions that affect you.

Government and other regulated customer data receives heightened protection and is excluded from any cross-customer use by default.

Citizen Data — information submitted by members of the public to our agency customers — is processed only to provide the contracted service and is not used to train AI models absent the agency customer’s express written authorization.

Every AI tool that touches customer data is reviewed and approved before deployment, and is bound by contractual data-protection obligations.

2. Scope of This Policy

This policy applies to our use of AI across two broad categories:

- Internal operations — how we use AI tools to run our business and to support and serve you (for example, in customer support, security operations, and back-office functions).
- Products and services — how AI capabilities are built into, or made available through, the products and services we provide to you.

It covers AI systems we develop ourselves and AI services we obtain from third-party providers, whether those services are cloud-hosted or operated within our environment. It does not change or override the specific commitments in your contract with us; where your agreement, any data processing addendum, or an applicable government contract sets stricter terms, those terms govern.

3. Our Responsible AI Principles

All use of AI at our company is governed by the following principles. These principles guide every decision about whether and how to deploy an AI tool or feature.

Principle	What it means in practice
Human oversight	AI supports human judgment; it does not replace it. People remain accountable for decisions, and AI output that affects customers is reviewed by a qualified person before it is acted upon.
Transparency	We are open about where and how we use AI, including disclosing AI service providers as sub-processors and telling you when AI is materially involved in a service you receive.
Privacy & data protection	We apply the same data-classification, consent, and contractual controls to AI that we apply across our business, and we limit AI access to data based on sensitivity and authorization.
Fairness	We take reasonable steps to identify and reduce the risk of unfair or biased outcomes, particularly where AI output could affect individuals.
Security	AI systems and the data flowing through them are protected by the same security program that protects the rest of our environment, including encryption and access controls.
Accountability & governance	A cross-functional review function approves AI use cases, maintains a registry of approved uses, and monitors them over time.
Lawfulness	We use AI in compliance with applicable laws, contractual obligations, and the procurement frameworks under which we serve government and regulated customers.

4. How We Use AI Internally

We use AI tools to operate our business more effectively and to improve the service you receive — including to market our solutions, support our customers, and deploy their implementations — and we continue to expand our use cases under the governance described in this policy.

Typical internal uses include:

- Customer support — helping our support team diagnose issues faster by analyzing support tickets, relevant product documentation, and (where appropriate) your instance configuration to suggest possible resolutions.
- Deployment and implementation — assisting our delivery teams in configuring, migrating, testing, and deploying your solution, subject to your contract and the data protections described in Sections 6 and 9.
- Marketing and communications — helping create and refine marketing content, campaigns, and communications. Customer data and Citizen Data are not used for marketing purposes without express authorization.

- Security and reliability — detecting anomalies, supporting monitoring, and helping us respond to potential threats.
- Productivity and back-office functions — assisting with drafting, summarizing, research, and analysis in functions such as sales operations, marketing, and administration.

In every internal use case, the following controls apply:

- Data is classified before it is used with any AI tool, and the most sensitive data is subject to the strictest controls and approvals.
- AI suggestions used in customer-facing contexts — such as support responses — are reviewed by a qualified employee before anything is communicated to you. The AI is a decision-support tool, not an autonomous decision-maker.
- Approved internal AI tools that process customer or other non-public data are bound by data-protection agreements that prohibit the provider from using that data to train its models.

Cross-customer learning

Some support tools can draw on knowledge gained from previously resolved issues to suggest faster resolutions. Where any such capability uses information derived from other customers, we apply strict controls: government and regulated-customer data is excluded by default, appropriate de-identification is applied, and the underlying data is never exposed across customer boundaries.

Any such capability operates within the commitments of the Accela AI Product Specific Terms — including the prohibition on using your data to train models shared across customers — and otherwise only as permitted under your agreement with us. Please contact us using the details in Section 13 with any questions.

5. How AI Is Used in Our Products and Services

Where AI capabilities are built into the products and services we provide, we design them to assist your team and to keep your organization in control. Depending on the features you use, AI may help with tasks such as summarizing information, suggesting responses, surfacing relevant records, or automating routine steps in a workflow.

When AI features are materially involved in a product you use, we will make that clear through product documentation, in-product notices, or your contract, so that you and your users understand when AI is assisting. Where a feature produces output for your review, your team remains responsible for evaluating that output before relying on it. The binding terms governing AI functionality in our products are the Accela AI Product Specific Terms, available at www.accela.com/terms/.

Automated decision-making

Our AI features are designed as decision-support tools. They do not make legally significant or similarly important decisions about individuals on a fully automated basis without meaningful human involvement. Where any feature could approach that threshold, we provide appropriate notice and, where required by law, mechanisms for human review.

6. Your Data and AI

Protecting your data is central to how we use AI. The following commitments apply to customer data processed in connection with any AI tool or feature.

6.1 We do not train foundation models on your data

We do not use your data to train, fine-tune, or otherwise improve third-party or publicly available AI models. Our agreements with AI service providers prohibit them from using customer data we send them for any purpose other than providing the contracted service to us, and specifically prohibit training the provider's models on that data.

6.2 Purpose limitation

Customer data is used with AI only for the purpose of providing and improving the service you receive — such as resolving your support request or operating a feature you use — and not for unrelated purposes.

6.3 Data isolation

We maintain controls designed to prevent one customer's data from being exposed to, or surfaced in the AI output delivered to, another customer.

6.4 Data minimization and retention

We limit the data made available to AI tools to what is reasonably necessary for the relevant purpose, and we retain data processed by AI systems in line with our standard retention practices and your contract. When data is deleted or your contract ends, data held by our AI service providers is deleted within a defined period.

6.5 What we do not do

- We do not sell your data.
- We do not allow AI providers to use your data to build or improve their general-purpose models.
- We do not use government or regulated-customer data for cross-customer purposes except where the relevant contract expressly authorizes it.

6.6 Citizen Data — information submitted by members of the public

“Citizen Data” means data loaded or submitted by individuals interacting with our agency customers — for example, when submitting permitting applications, applying for licenses, or submitting other information. It does not include information submitted by Authorized Users who are employees of the agency customer, except to the extent it incorporates Citizen Data, and then only to that limited extent. Information loaded or submitted by the agency customer or its Authorized Users, excluding Citizen Data, is “Agency Data.”

Because Citizen Data is entrusted to our agency customers by the members of the public they serve, we process Citizen Data with AI only under all of the following conditions:

- Contractual authorization — the processing is permitted under our agreement with the agency customer, including any data processing or AI-related terms.
- Consent and notice — legally required notices to, and consents from, the individuals concerned have been addressed, in most cases by the agency customer under its contract with us.
- No AI model training — we do not use Citizen Data to train, fine-tune, or improve any AI model, ours or a third party’s, even in aggregated or de-identified form, absent the agency customer’s express written authorization.
- Purpose limitation — Citizen Data is processed only to provide the contracted services to the relevant agency customer, and never for marketing or cross-customer purposes.
- Data minimization — we limit the Citizen Data made available to AI tools to what is reasonably necessary, preferring de-identified or synthetic data where feasible.
- Security — Citizen Data is processed only in environments protected by encryption, role-based access controls, and logging, and in accordance with applicable data residency and sovereignty commitments.
- Human oversight — AI output derived from Citizen Data that could affect an individual receives human review, and we do not use AI to make automated decisions about individuals.
- Approved sub-processors only — any AI provider that processes Citizen Data is bound by written obligations at least as protective as our commitments to you.
- Retention and deletion — Citizen Data processed by AI systems is retained and deleted in line with your contract and our standard retention practices.

7. Human Oversight and Accountability

We treat AI as a tool that supports our people, not one that replaces their judgment. Wherever AI output could affect you, a qualified person reviews and is accountable for the result before it is acted upon. Our staff are trained to understand the limitations of AI — including the possibility of incorrect or incomplete output — and to apply appropriate professional judgment rather than accept AI suggestions uncritically.

8. Third-Party AI Providers and Sub-Processors

Some AI capabilities rely on trusted third-party providers. Before any such provider processes customer data, we require contractual data-protection commitments, including:

- Purpose limitation — the provider may use the data only to deliver the contracted service to us.
- No model training — the provider may not use customer data to train or improve its models.
- Confidentiality, security, and breach-notification obligations.
- Deletion of customer data on termination or upon a valid deletion request.

Where AI providers act as sub-processors, we identify them in our sub-processor disclosures so that you can see who is involved in processing your data. We notify customers of changes in line with the process set out in your agreement (including any data processing addendum).

9. Protections for Government and Regulated Customers

A significant part of our business involves government agencies and other regulated organizations whose data is subject to specific statutory, contractual, and procurement-framework restrictions. We apply heightened protections to this data:

- Government and regulated-customer data is excluded by default from any cross-customer AI use, including any cross-customer learning described in Section 4.
- Such data is used only as permitted by the applicable contract and procurement framework, and only to provide the contracted service.
- Where a procurement vehicle or regulation requires it, additional controls — such as data segregation, residency, or restrictions on sub-processors — are applied.

If your organization is subject to a specific framework or regulation, please refer to your contract or contact us; the terms of that contract govern where they are stricter than this policy.

10. Security and Data Protection

AI systems and the data that flows through them are protected by the same information-security program that protects the rest of our environment. This includes encryption of data in transit and at rest, access controls that limit who and what can reach sensitive data, logging and monitoring, and incident-response procedures. For details of our security practices, please contact us.

11. Privacy and Your Rights

Our use of AI is consistent with our Privacy Policy (accela.com/privacy-policy) and applicable data-protection laws. Depending on your jurisdiction and your relationship with us, you or the individuals whose data we process may have rights regarding personal data — including rights of access, correction, and deletion, and rights relating to certain automated processing. We provide mechanisms to exercise these rights as described in our Privacy Policy and your contract. Where applicable law provides a right to opt out of certain automated processing, we honor valid requests.

12. Governance and Continuous Oversight

Our use of AI is overseen by our AI Committee, working with the Legal, Security, and IT Departments, under our internal AI Tools Usage Policy. Before an AI tool or use case that touches customer data is deployed, it is reviewed and approved against our internal AI governance standards. Approved use cases are recorded and monitored over time, and our standards are updated as technology, best practice, and regulation evolve. We align our program with recognized responsible-AI frameworks and applicable legal requirements.

13. Contact Us and Changes to This Policy

We may update this policy from time to time to reflect changes in our practices, technology, or legal obligations. When we make material changes, we will update the version and effective date above and, where appropriate, notify customers. The current version is always available at www.accela.com/terms/ and upon request.

14. Key Terms

Term	Meaning
Artificial intelligence (AI)	Computer systems that perform tasks — such as analyzing text, generating suggestions, or recognizing patterns — that would otherwise require human intelligence.
Foundation model	A large, general-purpose AI model trained on broad datasets that can be adapted to many tasks. We do not use your data to train these models.
Decision-support tool	An AI capability that provides suggestions or analysis for a person to review, rather than making decisions on its own.
Sub-processor	A third party we engage to process data on our behalf, including certain AI service providers.
De-identification	The process of removing or obscuring information that could identify a specific individual or organization.
Citizen Data	Data loaded or submitted by individuals interacting with our agency

Term	Meaning
	customers (e.g., permit applications, license applications, and other submissions). It excludes information submitted by agency-employee Authorized Users, except to the limited extent it incorporates Citizen Data.
Cross-customer use	Any use of information derived from one customer to benefit the service provided to other customers. Government and regulated-customer data is excluded by default.

This document is provided for transparency and informational purposes. It does not form part of any contract unless expressly incorporated by reference, and it does not modify the terms of your agreement with us. Where your contract, any data processing addendum, or an applicable government contract provides stricter protections, those terms govern.