LENDINGWISE

AI Governance & Data Protection Policy

Version 1.2 · Effective November 9, 2026 · Supersedes Version 1.1 (October 30, 2026) · Owner: Chris Fuelling, Chief Executive Officer

This policy explains how LendingWise (The Loan Post, Inc., dba LendingWise) uses artificial intelligence (AI), which AI providers receive client data, what is stored after processing, how that data is protected, and how we tell clients about a security incident. It is written for the security, vendor-risk, and compliance teams of organizations that use or are evaluating the LendingWise platform.

Answers at a glance

Is our platform data shared with third-party AI providers?	Only what you choose to send. The AI Document Review Agent reviews only the required document items you have enabled for AI review, and only on the loans you choose. For each of those documents, the document and the review rules your team set for it are sent to Amazon Web Services (AWS) and OpenAI for processing. Nothing else in the platform is sent to an AI provider, and if you leave the AI Agent off, none of your data is.
Which AI providers does LendingWise use?	Two enterprise AI platforms: Amazon Bedrock on AWS (Anthropic Claude models), plus Amazon Textract for text recognition, and OpenAI's business API, which we call directly (GPT-5.2 and GPT-4o). Amazon Bedrock is our strategic AI platform, and we are moving more of our AI processing onto it. We do not use Azure OpenAI, Google Gemini, or consumer AI products.
Is our data used to train AI models?	No. LendingWise does not train or fine-tune any model on client data, and our providers' business terms prohibit them from using it for training.
Does our data stay isolated to our organization?	Yes. Every document and AI result is tied to your organization's account. Each AI request contains one organization's data only. Your data is never pooled with other customers' data or used to benefit other customers.
Are prompts, documents, or interactions stored after processing?	LendingWise keeps the AI result (extracted data and the pass, fail, or needs-review finding) with your loan file. The working copy of each document sent for AI processing is deleted automatically after 30 days. LendingWise does not keep a separate log of prompts. OpenAI may keep API data for up to 30 days for abuse monitoring, and Amazon Bedrock does not store it. See Section 6.
Does LendingWise have a Zero Data Retention agreement with OpenAI?	No. LendingWise uses OpenAI's standard business API terms, under which OpenAI does not train on API data and may keep it for up to 30 days for abuse monitoring, then deletes it. If your organization requires different retention terms, you can use your own OpenAI API key, so AI processing runs under your own OpenAI account and agreement. See Section 2.

What security controls and certifications are in place?	Our security program is aligned with SOC 2 controls and is backed by a full set of written security policies. Controls include encryption in transit and at rest, US hosting on AWS, per-organization data isolation, role-based access, 30-day database backups, and audit logging. Full details are available through the LendingWise Trust Center. See Section 8.
How will we be told about a security incident?	If we confirm a security incident that affects your data, including data held by one of our AI providers or other sub-processors, we notify your organization without undue delay and no later than 72 hours after confirming it. We tell you what happened, what data is affected, what we have done, and what you should do, and we keep you updated until it is resolved. See Section 9.
Can our data be excluded from training or product improvement?	It already is, for every client, by default. There is nothing to request from LendingWise. You also control AI use directly: turn the AI Agent on or off yourself at any time, choose which documents it reviews, or use your own OpenAI API key (Section 12).

1. Scope

This policy covers two kinds of AI use, which we govern separately because they handle data differently:

- **In-product AI features.** AI features inside the LendingWise platform that your users interact with. Today this is the **AI Document Review Agent**, which reads documents uploaded to a loan file, extracts key data, and checks each document against the conditions your organization sets. Any future AI feature will follow this policy.
- **Internal engineering AI tools.** AI coding assistants that LendingWise engineers use to build and maintain the platform (Section 11).

Section 9 (security incidents and client notification) applies to all client data on the LendingWise platform, not only data used with AI.

2. AI providers (sub-processors)

LendingWise uses two enterprise AI platforms: **Amazon Bedrock** on AWS, and **OpenAI's business API**, which we call directly. Amazon Bedrock is our strategic AI platform. It runs inside the same AWS environment that hosts the LendingWise platform, and we are moving more of our AI processing onto it over time. We treat every AI provider as a sub-processor, and each is used under a business or enterprise agreement, never a free or consumer tier.

Provider	What it does	Models	Training on client data	Retention by the provider
Amazon Bedrock (AWS)	Interprets the review conditions your administrators write, and supports rule setup and testing	Anthropic Claude Sonnet 4.6 and Claude Haiku 4.5	Not used, and not shared with Anthropic	Not stored. LendingWise has Bedrock prompt logging turned off.
Amazon Textract (AWS)	Reads text from scanned documents (OCR)	—	Not used. LendingWise has opted out of AWS AI service improvement.	Held only long enough to return results to LendingWise

Provider	What it does	Models	Training on client data	Retention by the provider
OpenAI Business API, called directly from LendingWise's own OpenAI account	Classifies documents, extracts data, checks your conditions, and compares data across documents	GPT-5.2, GPT-4o	Not used. OpenAI does not train on business API data.	Up to 30 days for abuse monitoring, then deleted. No Zero Data Retention agreement.

The LendingWise platform and the AWS services above run in AWS data centers in the United States (US East, Ohio). Claude models are called through US-only Bedrock inference profiles, so those requests stay in US regions. We will not add an AI provider that processes client data without updating this list and notifying clients in advance (Section 12).

OpenAI data retention. LendingWise does not have a Zero Data Retention (ZDR) agreement with OpenAI. We use OpenAI's standard business API terms: OpenAI does not use API data for training, and it may keep API inputs and outputs for up to 30 days to detect abuse, after which they are deleted. That copy is held by OpenAI under its own security controls (OpenAI's API platform has a SOC 2 Type 2 report) and is covered by our incident notification commitment in Section 9. If your organization needs different retention terms, you can use your own OpenAI API key, so AI processing of your documents runs under your own OpenAI account and whatever agreement you have with OpenAI, or you can turn the AI Agent off (Section 12).

3. What data is shared with AI providers, and when

We want our clients to choose what they share with AI, at all times. You decide whether AI is used, which documents it sees, and whose account it runs under.

- **You choose the loans and documents.** The AI Agent reviews uploaded documents one required document item at a time. It reviews only the required document items you have enabled for AI review, and only on the loans you choose. Documents you have not enabled for AI review are never sent to an AI provider.
- **You choose whether AI runs at all.** Your team can turn the AI Agent on or off at any time, without contacting LendingWise. While it is off, nothing is sent to an AI provider.
- **You choose the account it runs under.** If you use your own API key, AI processing of your documents runs under your own OpenAI account and agreement.
- **Only what the task needs.** For each document reviewed, we send the document, its document type, the conditions and required fields your team set for it, and any loan-file fields a check needs. We do not send other loan files or other customers' data.
- **Always encrypted.** Data travels to every AI provider over encrypted (TLS) connections.
- **AI tools you connect yourself.** If your organization connects its own AI assistant to LendingWise through our API or connector, the data that assistant retrieves goes to the provider you chose, under your agreement with that provider.

4. Personal information (PII) and AI

Many loan documents consist largely of personal information, so when the AI Agent reviews a document you've enabled, it reads the PII in that document. Some checks, such as matching a borrower's name across an ID, a bank statement, and the loan file, can't be done without it. We protect that PII with these rules: it is sent only for the documents and loans you enable, encrypted in transit and at rest, never used for training, and shared only with the AI providers named in Section 2. AI features that act on your behalf, such as ordering third-party services, will use identifiers rather than raw PII wherever possible, and each order will require a user's approval.

5. Data isolation

- Every document, AI result, and AI configuration is stored with your organization's account ID and can be accessed only by your organization's authorized users and by LendingWise staff who need it to support you.
- Each AI request contains one document from one organization. We do not combine customers' data in a request.
- We do not build shared datasets, shared indexes, or models from customer data. What the AI learns from reviewing your documents is not used to improve results for any other customer.

6. Data retention for AI processing

Data	Where it is kept	How long
Documents you upload	LendingWise encrypted document storage	For the life of your account, under your control. Using AI does not change this.
Working copy of a document sent for AI processing	A separate, encrypted AI storage area on AWS (US)	Deleted automatically after 30 days. Any earlier versions are deleted 7 days after that.
AI results: extracted data, pass, fail, or needs-review findings, and validation reports	LendingWise database and encrypted storage, tagged to your organization	Kept with the loan file so your team can see how each document was reviewed, and handled under your client agreement and the LendingWise Data Retention Policy
Usage records: model used, page and token counts, processing time, cost	LendingWise database	Kept for billing and audit. They contain no document content.
Prompts and raw inputs sent to models	Not kept as a separate record by LendingWise. Bedrock prompt logging is off.	Not retained
AI service operational logs (status, errors)	AWS CloudWatch (US)	30 days
Data held by AI providers	AWS, OpenAI	Amazon Bedrock: not stored. Amazon Textract: only long enough to return results. OpenAI: up to 30 days for abuse monitoring, then deleted (standard API terms; no Zero Data Retention agreement).

When a client relationship ends, client data, including AI results, is returned or deleted as set out in the client agreement and the LendingWise Data Retention Policy.

7. Training and product improvement

- LendingWise does not train, fine-tune, or otherwise build AI models with client data.
- Amazon Bedrock does not use prompts or outputs for training and does not share them with model makers. LendingWise has opted out of AWS using Textract content to improve its services. OpenAI does not use business API data for training.
- LendingWise does not use client documents to build AI test or evaluation sets without the client's written permission. We use usage records (counts, timing, cost) to run and price the service.
- These exclusions apply to every client by default. No opt-out request is needed.

8. Security controls and compliance

- **Hosting.** The platform runs on Amazon Web Services in the United States (US East, Ohio).
- **Encryption in transit.** All connections to the platform, and from the platform to AI providers, use TLS.
- **Encryption at rest.** Production databases, document storage, and AI storage are encrypted. AI storage uses AWS Key Management Service (KMS) keys and blocks all public access.
- **Access control.** Role-based permissions in the application, two-factor authentication available to every user, and least-privilege access for LendingWise staff.
- **Secrets.** AI provider API keys are stored in AWS Secrets Manager, not in application code.
- **Backups.** Automated production database backups are kept for 30 days.
- **Audit logging.** AWS account activity is recorded with AWS CloudTrail and kept for one year.

Compliance standards. The LendingWise security program is aligned with SOC 2 controls and is designed to support clients' obligations under the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule. It is documented in a full set of written policies: Information Security, Data Classification, Data Retention, System Access Control, Password, Acceptable Use, Application Development Security, Change Management, Asset Management, Backup, Vulnerability Management, Security Incident Response, Human Resource Security, and Business Continuity and Disaster Recovery. Our infrastructure and AI providers maintain their own independent audits: AWS holds SOC 1, SOC 2, and ISO 27001 reports, and OpenAI's API platform has a SOC 2 Type 2 report.

Trust Center. The LendingWise Trust Center provides full disclosure for information security requests, including our policies and security documentation: **lendingwise.trustshare.com**.

9. Security incidents and client notification

Our internal Security Incident Response Policy covers how LendingWise detects, contains, investigates, and recovers from an incident. This section sets out what clients can expect from us when an incident affects their data.

- **What we notify you about.** Any confirmed security incident that results in unauthorized access to, or the loss, disclosure, or alteration of, your organization's data on the LendingWise platform. This includes data held by an AI provider or other sub-processor on our behalf.
- **When.** Without undue delay, and no later than **72 hours** after LendingWise confirms the incident. If a sub-processor tells us of an incident affecting your data, the same 72 hours apply from the time we confirm your data is involved. We do not wait for the investigation to finish before telling you.
- **How.** By email to your organization's primary account contacts and any security contact you have given us, followed by a call from your LendingWise account team. To name or change your security contact, email privacy@lendingwise.com.
- **What the notice includes.** What happened and when; which of your data and users are, or may be, affected; what we have done to contain it; what we recommend you do; and a named LendingWise contact. Where details are not yet known, we say so and send them as we confirm them.
- **Updates and closing report.** We send updates as the investigation progresses. When it is closed, we send a written summary of the cause, the impact, and the steps we have taken to prevent it from happening again.
- **Your notification obligations.** You own the relationship with your borrowers. We give you the information and cooperation you need to meet your own notification obligations to borrowers, regulators, and investors, including under the GLBA Safeguards Rule and state breach-notification laws. We coordinate with you before any notice is sent to your borrowers, unless the law requires us to send it directly.
- **Law enforcement.** If a law enforcement agency asks us in writing to delay notice, we may do so for the period the agency requires, and we notify you as soon as that period ends.
- **Reporting a suspected incident.** If you suspect a security issue involving LendingWise, such as a compromised user account, report it right away to privacy@lendingwise.com or your LendingWise account team.

10. Human oversight

AI supports decisions. It does not make them. The AI Document Review Agent gives a recommendation for each document: pass, fail, or needs human review. No AI output approves, denies, or prices a loan, or takes an adverse action, without a person reviewing it and acting on it. Your staff can review and override every AI result.

11. Internal engineering AI tools

- LendingWise engineers use AI coding assistants, such as Anthropic Claude Code, OpenAI Codex, and GitHub Copilot, to write, review, and test platform code. These tools are used under business or API terms that do not allow training on our inputs.
- Staff must not paste client personal or financial information, loan documents, or production data exports into any AI tool. Client data is processed by AI only through the in-product features described in this policy.
- All AI-assisted code goes through code review and testing before it is released to production.

12. Your controls

You decide how your organization uses AI, and you do not need to ask LendingWise to change it.

- **Turn the AI Agent on or off.** Your team can turn the AI Agent on or off in LendingWise at any time. Turning it off stops all AI processing of your data from that moment.
- **Choose what it reviews.** You choose which required document items the AI Agent reviews, and on which loans. Everything else stays out of AI processing.
- **Use your own API key.** You can use your own OpenAI API key, so AI processing of your documents runs under your own OpenAI account and agreement.
- **Know who processes your data.** Our current AI providers are listed in Section 2, and you can request their data-handling terms at any time.
- **Advance notice.** We will tell clients in advance of any material change in how client data is used with AI, such as a new AI provider or a new AI feature that processes loan data.
- **Questions and audits.** Security documentation is available through the LendingWise Trust Center (lendingwise.trustshare.com). Send other questions, security questionnaires, or audit requests to the contact below.

13. Policy governance

- **Owner:** Chris Fuelling, Chief Executive Officer, who is accountable for this policy and its enforcement.
- **Review:** at least once a year, and whenever we add an AI provider, model, or in-product AI feature.
- **Version history:** 1.0 (July 1, 2026), first release. 1.1 (October 30, 2026): names each AI provider and how it is used, and adds client controls, PII handling, retention, isolation, training, and compliance details. 1.2 (November 9, 2026): states that LendingWise has no Zero Data Retention agreement with OpenAI, and adds the client security-incident notification commitment (Section 9).

Contact. For questions about this policy, data handling, security incidents, or to request our current AI sub-processor list: privacy@lendingwise.com · Trust Center: lendingwise.trustshare.com