COALFIRE

AI GOVERNANCE AND TRANSPARENCY

AI transparency FAQ

Clear answers about how Coalfire governs artificial intelligence, protects customer data, honors customer requirements, and keeps qualified people accountable for customer-facing work.

AUDIENCE	SCOPE	LAST UPDATED
Customers and partners	Coalfire operations, services, and selected product capabilities	October 16, 2026

Our position

Coalfire uses AI within defined governance, security, privacy, and human-review controls. Customer commitments and documented restrictions govern before AI is used in connection with customer work.

APPROVED USE	CUSTOMER CONTROL	HUMAN ACCOUNTABILITY
Approved tools and approved workflows only	Contractual and engagement requirements come first	Qualified review before customer-facing delivery

About this FAQ: These answers describe Coalfire's general approach. The applicable agreement, engagement terms, customer requirements, and product documentation govern a specific engagement or service.

IN THIS FAQ

- Approach and use
- Customer data and restrictions
- Controls and oversight
- Products and services
- Frameworks and support

01 Approach and use

Coalfire evaluates AI use by tool, workflow, data, customer requirements, and the level of human oversight.

What is Coalfire's approach to using AI?

Coalfire uses AI to support selected business operations, service-delivery activities, and product capabilities. We permit use only through approved tools and approved workflows, with controls based on the data and the intended use.

AI does not replace human accountability or create an exception to contractual requirements, customer restrictions, security controls, or applicable law.

Does Coalfire use AI when providing services?

Coalfire may use AI to assist with approved service-delivery activities when the applicable agreement, engagement terms, customer requirements, and data-handling rules permit it.

A qualified professional reviews AI-assisted customer deliverables before delivery and remains accountable for the final work product.

Does approval of an AI platform approve every feature or workflow?

No. Coalfire evaluates tools, features, connectors, agents, integrations, and workflows for their intended use. Approval of a base platform does not automatically approve every capability or data flow within that platform.

02 Customer data and restrictions

Coalfire limits AI use to approved contexts and applies customer commitments before general platform approval.

Does Coalfire use customer data to train AI models?

Coalfire does not use customer data to train, fine-tune, reinforce, or otherwise improve AI models unless that use receives explicit written authorization and satisfies the applicable contractual, regulatory, engagement-specific, and customer requirements.

How does Coalfire protect customer data used in an approved AI workflow?

Coalfire applies data classification, minimum-necessary use, access control, approved-environment, and human-review requirements. Customer confidential or regulated data may be used only when the tool, workflow, and use case are approved and no customer restriction prohibits the use.

Coalfire prohibits personnel from entering credentials, secrets, tokens, or keys into AI tools.

Can a customer restrict or opt out of AI use?

Yes. Coalfire honors applicable contractual, engagement-specific, and documented customer restrictions on AI use. Customers may request an AI restriction or opt-out through their engagement contact or Coalfire's Compliance team.

Coalfire reviews the requested scope and documents the applicable restriction through the engagement process. A restriction may affect the delivery approach, schedule, or commercial terms, which Coalfire will address with the customer before proceeding.

How does Coalfire handle AI use in a customer-managed environment?

Coalfire's AI requirements continue to apply when our personnel work in a customer-managed environment. The customer's policies, contractual terms, and environment-specific restrictions also apply. When requirements differ, Coalfire follows the stricter requirement.

Customer data and AI interaction records remain within the customer-managed environment unless the customer explicitly authorizes a transfer and Coalfire completes any required internal approval.

How does Coalfire log and retain AI interactions?

Approved AI platforms may log prompts, outputs, and agent activity for security monitoring, compliance review, incident response, quality assurance, and audit purposes. Coalfire limits access to authorized personnel and applies retention requirements for the applicable platform, workflow, and engagement.

Customers may request engagement-specific retention information through their engagement contact or Coalfire's Compliance team.

03 Controls and oversight

Coalfire combines governance review, technical safeguards, customer restrictions, and qualified human accountability.

What safeguards govern Coalfire's use of AI?

Coalfire's safeguards include:

- approved tools, features, and workflows;
- data classification and minimum-necessary use;
- customer and engagement restriction checks;
- security, privacy, and supplier review based on risk;
- qualified human review of customer-facing output; and
- logging, monitoring, and incident response for approved environments.

Who is accountable for AI-assisted work?

The Coalfire professional using AI remains accountable for the data provided, the output produced, any actions taken, and the final work product. Coalfire requires qualified human review before AI-assisted content is delivered to a customer, regulator, or other external party.

Coalfire does not permit AI or AI-driven agents to make unsupervised decisions with legal, financial, employment, security, or customer impact.

How does Coalfire manage accuracy, bias, and other AI risks?

Coalfire limits AI to approved use cases and applies safeguards based on the data, workflow, and potential impact. Qualified personnel validate AI-assisted outputs for relevance, accuracy, and appropriate use before customer delivery.

Coalfire addresses AI risks through its broader security, privacy, supplier-risk, and incident-management processes. We review controls as technology, customer commitments, and regulatory expectations change.

How does Coalfire oversee third-party AI providers?

Coalfire permits only approved third-party AI tools, features, and workflows for customer work. The review considers the intended use, data handling, access, retention, model-training behavior, security, privacy, and applicable customer requirements.

Coalfire reevaluates approved use when a provider, capability, data flow, or risk profile changes materially.

04 Products and services

Product-specific controls and commitments are defined by the applicable product documentation and customer agreement.

What is Audit AI?

Audit AI refers to AI-enabled capabilities within Coalfire's Compliance Essentials platform that support selected compliance and documentation workflows. These capabilities operate within approved product architecture and remain subject to applicable customer agreements, product controls, and human oversight.

Coalfire does not use customer data to train the AI models used for these capabilities unless the customer provides explicit written authorization.

Can Coalfire help customers secure AI systems and agents?

Yes. Coalfire's AI Security and Trust Engineering practice helps organizations assess, design, build, and operate AI systems and agents with security and governance in mind. Services can address secure adoption, architecture, application security, automated security operations, and AI risk governance.

05 Frameworks and support

Coalfire uses recognized guidance while adapting controls to each use case and applicable obligation.

What frameworks inform Coalfire's AI governance?

Coalfire's AI governance approach is informed by recognized guidance, including the National Institute of Standards and Technology AI Risk Management Framework and the Open Worldwide Application Security Project guidance for large language model and generative AI applications.

Coalfire evaluates applicable regulatory and contractual requirements for the relevant customer, service, product, and jurisdiction. References to a framework describe guidance used by Coalfire and do not, by themselves, represent a certification.

Where can customers ask additional questions?

Customers can contact their Coalfire engagement team or email Compliance@coalfire.com for questions about AI governance, customer restrictions, consent, data handling, or engagement-specific requirements.

QUESTIONS ABOUT YOUR ENGAGEMENT?

Contact us

For additional information about Coalfire's AI governance, customer-specific restrictions, consent management, or engagement-specific requirements, contact our Compliance team or submit an inquiry through Coalfire's contact page.

Compliance@coalfire.com

Contact Coalfire

1 877-224-8077

Coalfire Systems, Inc.
330 North Wabash Avenue, Suite 1430
Chicago, Illinois 60611
Contact Coalfire · 1 877-224-8077

Copyright © 2026 Coalfire Systems, Inc.
All rights reserved.

Coalfire, the Coalfire logo, and Coalfire AI Security and Trust Engineering are trademarks or registered trademarks of Coalfire Systems, Inc. or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners.