COALFIRE

AI GOVERNANCE, SECURITY, AND TRANSPARENCY

AI transparency statement

Coalfire uses artificial intelligence under defined governance, security, privacy, and human-review controls. We apply security across identity, access, data, approved workflows, monitoring, and incident response while honoring customer-specific requirements and keeping 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

AI may assist Coalfire personnel, but it does not replace human accountability or create an exception to customer commitments, contractual requirements, security controls, or applicable law.

Our commitments · Governance · Security · Customer data · Training and model improvement · Customer restrictions · Human review and accountability

01

Our commitments

- **Approved use only.** Coalfire uses AI only through approved tools, approved features, and approved workflows.
- **Customer requirements first.** Customer-specific restrictions, contractual terms, engagement requirements, and regulatory obligations govern before AI is used on customer work.
- **Minimum-necessary data.** Coalfire classifies data before use and limits the data provided to an AI capability to what is needed for the approved purpose.
- **Human accountability.** Qualified personnel remain responsible for inputs, outputs, actions, and final work products.
- **No customer-data training by default.** Coalfire and customer data are not used to train, fine-tune, reinforce, or otherwise improve AI models unless explicitly approved in writing.
- **Reviewable activity.** Approved AI use is subject to logging, monitoring, and review for security, compliance, and incident-response purposes.

02

Governance

Coalfire uses AI in selected business operations, consulting and service-delivery workflows, and product capabilities, including Compliance Essentials and Hexeon. Each use remains subject to applicable governance, security, privacy, and customer requirements.

Coalfire governs AI use through formal policy, review, and approval processes with participation from security, legal, compliance, privacy, technology, and business stakeholders as appropriate.

Approval of a platform does not automatically approve every AI feature, connector, integration, agent, or workflow. Coalfire evaluates the specific use, data, workflow, and customer context before use is permitted.

Our approach emphasizes privacy, security, transparency, accuracy, fairness, explainability, and human oversight. It is informed by the NIST AI Risk Management Framework and considers applicable legal and regulatory requirements, including the European Union AI Act where relevant.

Coalfire also reviews the AI technologies it procures and monitors approved third-party AI use against applicable security, privacy, and responsible-use requirements.

03

Security by design and operation

Security is a distinct requirement in Coalfire's AI governance model. Coalfire permits AI for company work only through approved enterprise tools, features, connectors, and workflows evaluated for the intended data, access, and customer context.

Approved AI platforms use Coalfire-managed identity controls, including single sign-on and multi-factor authentication. Data connectors are reviewed before activation, access is limited according to least-privilege principles, and sensitive data sources require appropriate classification and approval.

Approved AI activity is logged and monitored to support security oversight, compliance review, investigations, and incident response. Access to sensitive AI interaction records is restricted to legitimate, governed purposes.

AI systems and agents do not receive unrestricted authority. High-impact or consequential actions require human approval, and suspected misuse, data exposure, or control failure is handled through Coalfire's formal security incident-response and escalation processes.

Security is applied throughout the AI lifecycle—from approval and access through monitoring and response.

04

Customer data protection

Customer confidential, restricted, or regulated data may be used only when the applicable AI tool, workflow, and use case are approved and no customer-specific restriction prohibits that use.

When Coalfire personnel work in a customer-managed environment, both Coalfire requirements and the customer's requirements apply. If they differ, Coalfire follows the stricter requirement.

Coalfire does not move customer data or related AI interaction records outside a customer-managed environment without explicit customer authorization and any required Coalfire approval.

05

Training and model improvement

Coalfire treats model training and model improvement as a separate approval decision. Customer data does not become eligible for training or fine-tuning because a tool is approved for another purpose.

Coalfire does not use customer data to train the AI models used in Compliance Essentials or Hexeon. If Coalfire proposes to use a third-party AI product that would train or improve a model using customer data, Coalfire will notify the customer in advance and complete any required consent, contractual review, and internal approval before that use.

Coalfire and customer data are not used to train, fine-tune, reinforce, or otherwise improve AI models unless explicitly approved in writing.

06

Customer-specific restrictions

Coalfire maintains a documented process for reviewing and maintaining customer-specific AI restrictions. Relevant contractual terms, security requirements, and engagement constraints are reviewed and applied through Coalfire's internal controls and engagement processes.

If a customer restriction prohibits AI use for an engagement or workflow, Coalfire does not use AI for that restricted purpose unless the governing condition changes through the applicable customer, contractual, or internal approval process.

Customers may request that AI not be used in services provided to them. Opt-out and consent-management requests may be directed to Compliance@coalfire.com.

07

Human review and accountability

AI-assisted content that will be delivered to a customer, regulator, or other external party must be reviewed by a qualified human before use. Coalfire does not permit AI or AI-driven agents to make unsupervised decisions on legal, financial, employment, security, or customer-impact matters.

Human accountability also applies to AI-enabled agents and automations. Coalfire requires a clear human owner, limits authority to the approved use, keeps outputs and actions reviewable, and requires human approval before high-impact actions execute.

FURTHER INFORMATION

Contact us

For additional information about Coalfire's AI governance, security, 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 and the Coalfire logo are trademarks or registered trademarks of Coalfire Systems, Inc. or its affiliates in the United States and other countries.