

AI Transparency Disclosures

Prepared by Aaron Ansel (Chief Artificial Intelligence Officer)

1. Purpose	4
2. AI Systems Overview.....	4
2.1 System Names:.....	4
2.2 Description	4
3. Intended Uses.....	4
3.1 Primary Objectives.....	4
3.2 Approved Use Cases	4
3.3 Prohibited Uses	5
4. Limitations and Ethical Considerations.....	5
4.1 Known Limitations	5
4.2 Ethical Considerations.....	5
5. Stakeholder Responsibilities	5
5.1 Development Team	5
5.2 Compliance Officer.....	5
5.3 Customer Service Team	5
6. Disclosure Statement	6
7. Performance Metrics and Error Types	6
7.1 Performance Metrics Definitions.....	6
7.2 Acceptable Error Ranges.....	6
8. Operational Factors and Critical Uses.....	6
8.1 Operational Context.....	6
8.2 Critical Context for Reliable Use	6
9. Sensitive Use Cases.....	7
10. Controls to Mitigate Automation Bias	7
11. System Limitations and Predictable Failures.....	7
12. Known AI Risks and Mitigations	8
13. Evidence of System Performance	8
14. Update and Notification Plan.....	8

14.1 Conditions Requiring Updates	8
14.2 Communication Process	8
15. Standard Operating Procedure (SOP) for System Health Monitoring	9
15.1 Reproducing System Failures	9
15.2 Monitoring Events	9
15.3 Third-Party AI Components	9
15.4 AI System Monitoring and Adaptation Framework.....	9
16. System Health Monitoring Methods.....	9
17. Policies for Failure of Intended Use	9
18. Supporting Evidence	10
19. Approval	10
20. Document Revision History	10

1. Purpose

The purpose of this document is to ensure transparency in the intended uses of AI systems developed by KYG Trade. It provides clear information about the objectives, limitations, and ethical considerations of each AI system, enabling stakeholders to make informed decisions.

2. AI Systems Overview

2.1 System Names:

- ChatHS (Harmonized Schedule classification for import)
- ChatECN (Export classification)
- Trade Prompt System (traceable document analysis)
 - ChatFTA (Free trade agreement qualification)
 - ChatFL (Forced labor supply chain risk assessment)
 - ChatFSE (First sale for export)
- Smart Screen (screening adjudication)

2.2 Description

These AI-powered applications (embedded inside KYG's Core Workflow system) are designed to assist customers with Classification codes for provided product attributes. The backend of this interface is a web API interface that leverages frontier LLMs through API, to perform RAG on various public data sources, and return the classification codes.

It must be noted that the AI engines process only industrial product attributes and do not rely on any customer data to provide AI inferences.

3. Intended Uses

3.1 Primary Objectives

- Automate routine product classification tasks to optimize human resource allocation.
- Gather relevant context and documentation to assist user with compliance-related decisions
- Facilitate supplier communication and collaboration
- Minimize analysis time and improve customer satisfaction.

3.2 Approved Use Cases

- Responding to Product classification related queries.
- Redirecting complex issues to human agents when a product classification code cannot be reasonably ascertained by AI.

3.3 Prohibited Uses

- Making decisions that require human judgment, such as approving loans or resolving sensitive disputes. Basically, for anything other than Product Classification purposes for which the AI systems are built.
- Collecting personal data beyond what is required for interaction.
- Engaging in activities outside the defined scope of customer service.

4. Limitations and Ethical Considerations

4.1 Known Limitations

- May fail to understand nuanced or ambiguous queries.
- Responses may be inaccurate if input data is incomplete or unclear.
- Cannot handle situations requiring empathy or complex reasoning. KYG AI applications are predominantly built to assist users in getting a product classified as accurately as possible, with minimal product attributes inputs.

4.2 Ethical Considerations

- Ensuring user data privacy and confidentiality.
- Avoiding biases in responses caused by training data. No foundation models are trained by KYG Trade, and only prompting and RAG (Retrieval Augmented Generation) are relied upon to obtain inferences.
- Informing users when they are interacting with an AI system.

5. Stakeholder Responsibilities

5.1 Development Team

- Ensure the AI system aligns with the organization's ethical AI guidelines.
- Conduct regular audits to monitor system performance and identify biases.

5.2 Compliance Officer

- Verify adherence to regulatory standards
- Maintain documentation of AI system assessments and updates.

5.3 Customer Service Team

- Monitor AI interactions and provide feedback for continuous improvement.
- Handle escalations promptly when the AI system is unable to resolve an issue.

6. Disclosure Statement

This AI system is designed to enhance product classification and assessment services by automating routine tasks involving lookup of various regulatory and compliance sources to determine product classification codes. While efforts have been made to ensure accuracy and reliability, the system is not a substitute for human expertise in complex or sensitive scenarios. Users interacting with this AI system will be informed about its automated nature at the start of the interaction.

7. Performance Metrics and Error Types

7.1 Performance Metrics Definitions

Accuracy: Percentage of correct outputs measured as consistency between determination logic and established context.

Latency: Response time for producing outputs.

Note – False Positive and False Negative rates are not considered because we do not train or fine-tune LLMs.

7.2 Acceptable Error Ranges

Operational Factor	Acceptable Error Range	Impact on Intended Use	Mitigation Strategies
Accuracy	95-100%	Critical for sensitive data analysis tasks.	Regular model assessment, validation.
Latency	<3 min.	Critical for real-time processing applications.	Optimize infrastructure and scaling.

8. Operational Factors and Critical Uses

8.1 Operational Context

The following factors impact AI system reliability:

Input Data Quality: Poor data inputs reduce performance accuracy.

System Environment: Performance depends on infrastructure health.

User Interaction: Misuse or incorrect inputs impact outputs.

8.2 Critical Context for Reliable Use

High-quality, clean input datasets are mandatory for optimal performance, including data obtained from third-party data providers.

AI models require a stable computational environment for intended use, including Frontier models hosted by third parties.

Systems must be tested in real-world conditions periodically to manage emerging risks and degradation in quality of determinations.

9. Sensitive Use Cases

For current AI solution offerings, KYG Trade has determined the intended use cases do NOT constitute sensitive use.

10. Controls to Mitigate Automation Bias

To discourage automation bias:

User Training: Users are trained to critically review AI outputs.

Explainable AI: System outputs include rationales for decision-making.

Alerts for Confidence Threshold: System flags results with low confidence scores.

11. System Limitations and Predictable Failures

Limitation	Impact	Mitigation
Limited Input Data	Reduces accuracy.	Periodic data updates and curation of data source used for RAG from external sources
Model Hallucinations	Incorrect outputs.	All LLM prompts in KYG applications are instructed to rely on data provided through RAG in the context window and not to use LLM's knowledge acquired during its training.
Data Bias	Discriminatory outputs.	Only products related data is processed, and no human-related information is processed by KYG's AI systems for inference.
System Downtime	Impacts reliability.	Automated failover and health monitoring.

12. Known AI Risks and Mitigations

Risk	Description	Mitigation Strategy
Inference Manipulation	Prompt exploits generating unintended results.	Input sanitization monitoring logs. Access to AI systems is restricted to KYG's Core application.
Model Manipulation	Data poisoning affecting model integrity.	We are not training or fine-tuning any LLMs for usage in our AI applications. We use hosted frontier models, access them through API, and rely on RAG and prompting for inference.
Inferential Disclosure	Prompt extraction exposing sensitive info.	Output filtering, access controls.

13. Evidence of System Performance

Performance Tests: Benchmarked system results across defined use cases.

Generalizability Reports: Testing models against diverse real-world datasets.

System Accuracy Evidence: Reported accuracy maintained over periodic testing.

14. Update and Notification Plan

14.1 Conditions Requiring Updates

KYG Trade, Inc. will update transparency disclosures when:

- New use cases are added.
- Functionality changes or new versions are released.
- New system performance or risk information is identified.

14.2 Communication Process

Notifications will be sent to customer via official email.

Updates will include versioned documentation, summary of changes, and effective dates. Contact:

Aslam Latheef

15. Standard Operating Procedure (SOP) for System Health Monitoring

15.1 Reproducing System Failures

All failures are logged, replicated, and tested in a controlled environment.

15.2 Monitoring Events

Event Type	Priority	Frequency of Review	Response Time
System Failures	High	Daily	Immediate (1-4 hours)
Model Hallucinations	Medium	Weekly	24-48 hours
Latency Issues	Medium	Weekly	24-48 hours

15.3 Third-Party AI Components

Open-source libraries and third-party components are updated monthly.
Logs are maintained to track component updates and version changes.

15.4 AI System Monitoring and Adaptation Framework

[Documented Here](#)

16. System Health Monitoring Methods

Data Repositories: Logs generated for errors, usage, and failures.

System Analytics: Tools like Prometheus and Grafana monitor system health.

Customer Feedback Submission: Clients can submit failures via support@kyg.ai.

Public Feedback: General public can report concerns to info@kyg.ai

17. Policies for Failure of Intended Use

In case an AI system fails to meet its intended use:

1. We will notify impacted customers immediately.
2. Remove the intended use from customer-facing materials.
3. Address identified issues and revise documentation.
4. Publish updated documentation with clear version history.

18. Supporting Evidence

Upon request, KYG Trade will provide:

1. Screenshots of system health monitoring dashboards.
2. Event logs, including system failures and mitigations.
3. Versioned updates of this transparency disclosure document.

19. Approval

This document has been reviewed and approved by the following individuals:

Name	Title	Signature	Date
Delsean Littlejohn	VP of Customer Success and Compliance Lead	Delsean Littlejohn	12-17-2024
Aaron Ansel	Chief AI Officer	Aaron Ansel	10-29-2025

20. Document Revision History

Date	Version	Description of Changes	Author
12-17-2024	1.0	Initial version	Aaron Ansel
10-29-2025	1.1	Updated models in use and changed company contact from Delsean to Aslam	Aaron Ansel

This document is a living policy and will be updated regularly to reflect advancements in AI technologies, regulatory changes, and organizational growth. Stakeholder feedback is encouraged to ensure the policy remains relevant and effective.

Addendum A: Frequently Asked Questions

1. Which AI models does KYG Trade use for its systems?

KYG Trade leverages industry-leading frontier Large Language Models (LLMs) provided by trusted third-party vendors, such as OpenAI. We typically use dedicated Azure deployments of these models, housed in the United States. Our systems do not train or fine-tune these LLMs; instead, they utilize retrieval-augmented generation (RAG) methods with publicly available and regulatory-specific datasets to provide accurate product classification. Specifically, we use the following models:

- Gpt-4.1
- Gpt-4.1-mini
- Gpt-5
- Gpt-5-mini
- Gpt-oss-120b

2. What data was used in the original training of these models?

The foundational LLMs we employ were trained by their providers on extensive, publicly available internet data, including books, websites, and licensed datasets. KYG Trade does not control or influence this initial training data but ensures that no customer-specific data is used in these foundational models.

3. Where is customer data stored when processed by KYG Trade's AI?

Customer inputs (utterances or product attributes) provided during interactions are temporarily processed in our application's short-term memory, strictly managed within KYG's secured environment. This data is never stored within the external LLMs. Once the workflow is completed, customer-specific session data is discarded promptly, ensuring minimal data retention.

4. How long is customer data retained by KYG Trade after an AI interaction?

Customer-specific data processed during AI interactions is retained only briefly, typically limited to the duration necessary to complete the specific workflow. Following this, the data is promptly deleted to minimize retention risks, except for regulatory resources or approved long-term data explicitly permitted by customers.

5. Does KYG Trade have a 'Right to Forget' policy for AI-generated data?

Yes. In alignment with data protection laws (GDPR, CCPA), customers have the right to request deletion of their data. Given our minimal retention policy, most data is immediately discarded post-processing, but we honor explicit deletion requests promptly, in compliance with applicable privacy regulations.

6. Is customer data used to further train KYG Trade's AI models?

No. KYG Trade does not use customer-specific data to train or improve foundational AI models. Any improvements or updates to our AI systems rely solely on publicly available data and carefully curated regulatory materials, ensuring customer privacy and data isolation.

7. What does KYG Trade's AI audit process entail?

Our AI audit process includes continuous monitoring of system performance metrics such as accuracy, latency, and reliability. Regular audits are performed to detect and address biases, inaccuracies, or security vulnerabilities. We utilize comprehensive logging and real-time monitoring tools (e.g., Prometheus and Grafana) to maintain transparency and accountability.

8. Does KYG Trade manually review individual AI interactions for accuracy?

Yes. Our customer service and compliance teams periodically perform random manual reviews of AI interactions to validate accuracy, relevance, and adherence to intended use. These reviews help identify areas for improvement and ensure our systems consistently meet performance standards.

9. What guardrails does KYG Trade have to prevent unauthorized or inappropriate use ("jailbreaking") of AI?

KYG Trade implements strict input validation, context isolation, role-based access controls, and comprehensive logging to mitigate risks such as prompt injection attacks and misuse. Additionally, system outputs are monitored, and alerts are configured for any anomalous behaviors or unauthorized activities.

10. Does KYG Trade assume liability for unauthorized AI system behavior?

KYG Trade provides AI solutions with robust security and control measures; however, per our AI Features Addendum, liability for unauthorized or inappropriate system behavior resulting from misuse or deliberate circumvention ("jailbreaking") by users is not assumed

by KYG Trade. We encourage users to follow prescribed guidelines and use the systems as intended.

11. What is KYG Trade’s history and experience with AI?

KYG Trade has been actively integrating and deploying Generative AI technologies since 2021, focusing extensively on regulatory compliance applications. Our AI leadership team, led by Chief AI Officer Aaron Ansel, brings substantial experience in developing and managing secure, reliable, and ethically robust AI systems aligned with global best practices.