

ARTIFICIAL INTELLIGENCE ACCEPTABLE USE POLICY

Last Updated: September 17, 2026

1. Scope

This Artificial Intelligence (“AI”) Acceptable Use Policy (“Policy”) is incorporated by reference into and forms part of the Master Services Agreement (“MSA”) and any applicable Order Form between ComplianceQuest, Inc. (“CQ”) and Customer.

In the event of a conflict, an expressly negotiated AI provision in an Order Form or the MSA will prevail over this Policy. This Policy will govern acceptable use of CQ AI Services.

This Policy applies to Customer’s use of all CQ services incorporating artificial intelligence, machine learning, generative AI, AI agents, copilots, and automation features, including productized third-party AI integrations (collectively, “CQ AI Services”). CQ AI Services are designed to assist users but not to replace human judgment. Customer is responsible for all use of CQ AI Services in accordance with this Policy and applicable laws.

By accessing or using the CQ AI Services, Customer agrees to be bound by the terms of this Policy. Customer is responsible for ensuring that its users comply with this Policy, and any use of the CQ AI Services by Customer or its users constitutes acceptance of and agreement to this Policy.

CQ may update this Policy from time to time by posting the updated Policy on CQ’s website at www.compliancequest.com. Customer’s continued use of the CQ AI Services following such updates constitutes acceptance of the revised Policy. CQ will provide reasonable notice of changes that materially reduce Customer’s rights or materially increase Customer’s obligations. Unless required earlier by applicable law or reasonably necessary to address an urgent security or misuse risk, material changes will become effective on the date stated in the notice. No update will retroactively alter the parties’ rights or obligations with respect to use occurring before the effective date of the update. A material violation of this Policy will constitute a material breach of the applicable MSA or governing agreement, subject to any applicable notice and cure rights. CQ may suspend access to affected CQ AI Services where reasonably necessary to prevent material harm, unlawful activity, a security threat, or continued violation of this Policy.

2. Definitions

“Customer Input” means data, prompts, instructions, content, or other information submitted to a CQ AI Service by or on behalf of Customer. “AI Output” means content, recommendations, summaries, classifications, predictions, or actions generated by a CQ AI Service in response to Customer Input. “AI Agent” means a CQ AI Service configured to plan, recommend, initiate, or execute actions through CQ or connected systems. “High-Impact Decision” means a decision that materially affects regulatory compliance, legal rights, health or safety, employment, education, housing, credit, access to public benefits, or another similarly consequential interest.

3. Responsible AI Principles

Customer agrees to use CQ AI Services in accordance with the following principles:

- Human Accountability: Humans remain responsible for AI Output and decisions based on AI Output.
- Fairness and Non-Discrimination: AI may not be used in ways that unlawfully discriminate.
- Transparency: Users must understand when they are interacting with AI.
- Safety and Reliability: AI Output must be reviewed and validated in a manner proportionate to the intended use and associated risk.
- Privacy and Security: Customer must protect personal and sensitive data.

4. Use of Customer Data

CQ may process Customer Data and Customer Input to provide, secure, support, configure, monitor, and improve CQ AI Services for Customer's use. CQ will not use Customer Data, Customer Input, or AI Output generated in response to Customer Input to train or fine-tune a model made generally available to other customers, or permit a third-party AI provider to do so, unless Customer expressly authorizes such use in writing. CQ AI Services may use third-party AI and infrastructure providers to deliver designated functionality. Applicable providers may vary by service, deployment, geography, and Customer configuration.

CQ shall not disclose Customer Data to third parties except as necessary to provide the CQ AI Services or as otherwise authorized by Customer. Customer Data, Customer Input, and AI Output generated in response to Customer Input shall be treated as confidential, without expanding any ownership or intellectual property rights in AI Output.

CQ may use aggregated or de-identified service telemetry that does not identify Customer, its users, or any individual to operate, secure, analyze, and improve CQ AI Services. CQ may use feedback voluntarily provided by Customer regarding CQ AI Services, provided that CQ does not disclose Customer Confidential Information or incorporate Customer Data into a generally available model without authorization.

Where supported by the applicable CQ AI Service and underlying provider, Customer may configure, disable, or opt out of designated AI features or designated provider data-use options. Available controls and associated limitations will be described in the applicable service documentation. Customer shall not submit personal, sensitive, regulated, export-controlled, or other restricted data to a CQ AI Service unless such data is permitted under the applicable MSA, Order Form, DPA, BAA, service documentation, and Customer configuration, and Customer has implemented required safeguards and obtained all necessary rights, notices, and consents.

5. Prohibited Uses

Customer shall not use CQ AI Services to:

- Knowingly generate or distribute materially false, deceptive, or misleading content for the purpose of defrauding, impersonating, manipulating, or causing material harm.
- Create or distribute synthetic media, including deepfakes, without appropriate authorization, consent, and disclosure.
- Violate laws, privacy rights, or intellectual property rights.
- Use AI Output as the sole basis for a High-Impact Decision without meaningful human review.
- Provide legal, financial, or medical advice without qualified human review.

- Circumvent, disable, interfere with, or bypass safety, security, access-control, usage-limit, or content-control mechanisms, or reverse engineer CQ AI Services except to the extent such restriction is prohibited by applicable law.
- Generate malicious code or exploits.
- Generate or distribute political advertising, election communications, or political persuasion content in violation of applicable election, campaign-finance, advertising, disclosure, or privacy laws.
- Generate explicit or exploitative content, including non-consensual imagery.
- Develop or support any lethal or weaponized function.
- Engage in social scoring, unlawful biometric categorization, prohibited emotion recognition, manipulation of vulnerable individuals, or any other AI practice prohibited by applicable law.
- Use CQ AI Services, Customer-accessible model interfaces, or outputs obtained through systematic extraction to train, replicate, or develop a competing AI model or service, except with CQ's prior written authorization.

6. Responsible Use Requirements

Customer must ensure human oversight, risk assessment, and validation of AI Output proportionate to the intended use and associated risk. Before deploying CQ AI Services in a consequential or regulated workflow, Customer must assess the nature of the data, affected individuals, reasonably foreseeable misuse, required accuracy, applicable legal requirements, and the consequences of an incorrect or unauthorized output or action. Where CQ AI Services assist in providing legal, financial, medical, or other regulated advice, a qualified professional must review and approve the output before reliance.

Human oversight must be meaningful and performed by a person with appropriate authority, competence, information, and opportunity to review, reject, correct, stop, or reverse an AI-generated recommendation or action before a High-Impact Decision is finalized.

Customer is responsible for all decisions made, advice given, actions taken, and failures to take action based on CQ AI Services.

Customer agrees to provide reasonable information regarding its intended use of CQ AI Services upon request.

7. Transparency and Disclosure

Customer must provide disclosures regarding AI interaction or AI-generated content where required by applicable law or reasonably necessary to avoid material deception. Customer must not knowingly misrepresent AI-generated content as human-generated where doing so would be materially misleading.

8. Security and Data Protection

Customer must implement appropriate identity, access, credential, endpoint, and data-security controls for CQ AI Services and safeguard sensitive and confidential data. Customer shall not expose credentials, tokens, confidential prompts, system instructions, or connected-system access to unauthorized persons. Customer must promptly notify CQ of suspected unauthorized access, harmful agent behavior, security bypass, material misuse, or unauthorized disclosure of Customer Data involving CQ AI Services and reasonably cooperate in containment and remediation.

9. AI Agents and Automation

Customer must configure AI Agents and automated workflows using least-privilege access, defined data and transaction boundaries, appropriate approval thresholds, and audit logging. Customer is responsible for agents and workflows that it configures, enables, deploys, or authorizes, including actions performed through connected systems. Customer must maintain appropriate human approval before an AI Agent performs a consequential, externally binding, irreversible, safety-related, or regulatory action. Customer must periodically review permissions and logs and promptly disable or contain an agent that behaves unexpectedly, exceeds its authority, presents a security risk, or violates this Policy.

10. High-Risk Use Disclaimer

CQ AI Services are not designed or intended to autonomously make or execute determinations that could reasonably result in death, serious bodily injury, catastrophic property damage, or material impairment of legal rights without appropriate safeguards and meaningful human oversight. Unless expressly stated in an applicable Order Form or service description, CQ AI Services are not designed, validated, or intended to function as a medical device, provide autonomous clinical decision support, or independently make final regulatory, quality, safety, legal, employment, credit, or other High-Impact Decisions. Nothing in this section prohibits Customer from using CQ AI Services to support quality, risk, compliance, regulatory, or safety processes, provided Customer maintains appropriate validation, procedural controls, human oversight, and responsibility for resulting decisions and actions.

11. Intellectual Property and AI Output

As between CQ and Customer, ownership of Customer Data remains governed by the MSA. CQ does not claim ownership of AI Output generated in response to Customer Input and made available to Customer through the CQ AI Services. Due to the probabilistic nature of AI services, the same or similar output may be generated for other users. CQ does not represent that AI Output is protectable, non-infringing, or suitable for Customer's intended use. Customer is responsible for any required review before publishing or commercially using AI Output.

12. Disclaimer of Liability

CQ AI Services produce probabilistic outputs that may be inaccurate, incomplete, non-unique, or unsuitable for a particular purpose. Customer is responsible for evaluating and validating AI Output in light of its intended use. To the maximum extent permitted by applicable law, and subject to the warranties, disclaimers, limitations of liability, indemnities, and exclusive remedies in the MSA, CQ is not responsible for Customer's failure to review AI Output, unauthorized configurations, misuse of CQ AI Services, or decisions made solely in reliance on AI Output.