[AGENCY NAME] ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE POLICY

Version: [1.0] Effective date: [DATE] Policy owner: [NAME, TITLE]
Next review date: [DATE, no more than six months after the effective date]

1. PURPOSE

This policy explains how [Agency Name] staff may use artificial intelligence tools in their work. Its goals are to protect client, carrier and agency information, to meet our legal and contractual duties, and to make sure a qualified person stays responsible for every piece of advice and every document we send.

2. SCOPE

This policy applies to every employee, producer, contractor and intern who does work for [Agency Name], on any device, whether owned by the agency or personally owned. It covers chat assistants, writing and summarizing tools, AI features built into agency software (such as the agency management system, email, CRM, quoting and enrollment platforms), meeting note-takers, and browser extensions.

3. DEFINITIONS

- "AI tool" means any software that generates text, images, code, summaries, or analysis from a prompt or from data it is given.
- "Approved AI tool" means a tool listed in Appendix A, used through an account that the agency controls.
- "Restricted data" means the information listed in Section 5.3.
- "Output" means anything an AI tool produces.

4. APPROVED TOOLS AND ACCOUNTS

4.1 Staff may use only the AI tools listed in Appendix A for agency work.

4.2 Agency work must be done in agency-controlled business accounts, never in personal or free consumer accounts.

4.3 Approved tools must be configured so that agency data is not used to improve the vendor's models, and data retention must match the settings recorded in Appendix A.

4.4 Staff may request a new tool from the Policy Owner. A tool is not approved until it has passed the vendor review in Section 8 and been added to Appendix A.

4.5 Meeting note-takers may be used only with the consent of every participant, and recordings that contain restricted data must be stored and deleted under our records policy.

5. DATA RULES

5.1 Green (allowed in approved tools): public information, agency marketing content, general insurance and benefits questions, and internal documents that contain no client data.

5.2 Yellow (allowed only in approved tools and only after masking): client business names, plan designs, rate exhibits, census files, loss runs, schedules of insurance and carrier quotes, once individual identifiers have been removed or replaced with placeholders.

5.3 Red (never entered into any AI tool, including approved tools, unless the Policy Owner has approved a specific workflow in writing and a business associate agreement or equivalent contract is in place):

- Social Security numbers, driver's license numbers, passport numbers and dates of birth tied to a name
- Protected health information, including diagnoses, claims detail, prescriptions and large-claimant reports that identify a person
- Bank account, credit card and payment information
- Usernames, passwords, and access codes for carrier or client systems
- Anything a client or carrier contract says may not be shared with third parties

5.4 When in doubt, treat the data as Red and ask the Policy Owner.

6. HUMAN REVIEW

6.1 A qualified staff member must review and approve every output before it is sent to a client, prospect, carrier or regulator, or used to make a coverage, eligibility, pricing or claims recommendation.

6.2 Staff must check figures, plan details, coverage terms, and dates against the source documents. AI tools can produce confident errors.

6.3 AI may not make final decisions about coverage, underwriting, claims, eligibility or employment.

6.4 The person who sends a document is responsible for its content, whether or not AI helped draft it.

7. CLIENT TRANSPARENCY

7.1 We will tell clients that we use AI tools to support our work when they ask, and in our [privacy notice / engagement letter].

7.2 We will honor any client request that their information not be processed with AI tools.

8. VENDOR REVIEW

Before a tool is approved, the Policy Owner will confirm and record:

- Where data is stored and how long it is kept
- Whether customer data is used to improve the vendor's models, and how to turn that off
- Whether the vendor will sign a business associate agreement (required for any workflow that touches PHI) and a data processing agreement
- Security certifications (for example SOC 2 Type II)

- Admin controls, including single sign-on, user removal, and audit logs
- How the vendor reports a security incident

9. REGULATORY ALIGNMENT

This policy is intended to support our obligations under [HIPAA, as applicable to our benefits work], the Gramm-Leach-Bliley Act, state insurance data security laws [list applicable states], and our carrier and client contracts. It is also written to meet the expectations in the NAIC Model Bulletin: Use of Artificial Intelligence Systems by Insurers (adopted by the NAIC on December 4, 2023) where a carrier contract or our state's adoption of that bulletin reaches this agency. The bulletin is addressed to licensed insurers, not to agencies.

10. INCIDENTS

10.1 Staff must report any suspected misuse, including Red data entered into any AI tool or agency data entered into an unapproved tool, to the Policy Owner within [24] hours.

10.2 The Policy Owner will assess the incident, contact the vendor to request deletion where possible, and follow our incident response plan, including any required client, carrier or regulator notice.

10.3 Reporting a mistake promptly will not by itself result in discipline.

11. ONBOARDING AND ACKNOWLEDGMENT

11.1 Every staff member will review this policy with their manager before receiving access to an approved tool, and annually after that.

11.2 Every staff member must sign the acknowledgment in Appendix B.

12. ENFORCEMENT

Violations may result in loss of tool access and disciplinary action, up to and including termination, consistent with our employee handbook.

13. REVIEW

The Policy Owner will review this policy at least every six months, and whenever we add a tool, change vendors or a relevant law changes.

APPENDIX A: APPROVED AI TOOLS

Tool	Account type	Approved uses	Data allowed (Green/Yellow)	Retention setting	BAA signed?	Approved by / date
[ ]	[Business]	[ ]	[ ]	[ ]	[Y/N]	[ ]

APPENDIX B: STAFF ACKNOWLEDGMENT

I have read the [Agency Name] AI Governance Policy, I understand it, and I agree to follow it. I understand that Red data must never be entered into an AI tool and that I am responsible for reviewing any AI output that I send.

Name: _____ Signature: _____ Date: _____