Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

AI GOVERNANCE SERVICE — SAMPLE POLICY DOCUMENT

AI Acceptable Use Policy — Sample

Approved Tools · Prohibited Uses · Client Disclosure · Enforcement

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

AI Acceptable Use Policy — Sample

About This Document

This is a sample AI Acceptable Use Policy developed by Axiom Sovereign. It is designed for professional services organizations — CPA firms, law firms, medical practices, and management consultancies — that handle sensitive client data and have professional ethics obligations. Bracketed fields must be completed for your specific organization. This sample should be reviewed by legal counsel before adoption. Axiom Sovereign develops customized, organization-specific AI governance policies as part of our AI Governance engagement.

Policy Title: Artificial Intelligence Acceptable Use Policy

Policy Number: [POL-AI-001]

Effective Date: [DATE]

Last Reviewed: [DATE]

Policy Owner: [NAME / TITLE]

Applies To: All employees, contractors, and authorized users of [ORGANIZATION NAME] systems

Review Cycle: Annual (or upon significant regulatory or technology change)

1. PURPOSE

[ORGANIZATION NAME] ("the Firm") is committed to enabling the productive use of artificial intelligence (AI) tools while protecting the confidentiality of client information, meeting our professional ethics obligations, and complying with applicable laws and regulations. This policy establishes the rules governing the use of AI tools by all Firm personnel.

2. SCOPE

This policy applies to all uses of AI tools by Firm personnel — including employees, contractors, and any other authorized users — when conducting Firm business or using Firm systems. It applies to AI tools used on Firm-owned devices, personal devices used for Firm business, and any AI-enabled features of software the Firm uses.

3. APPROVED AI TOOLS

The following AI tools are approved for use in connection with Firm business, subject to the restrictions in Section 5:

Tool Name	Version / Plan Required	Permitted Uses	Restrictions
Microsoft 365 Copilot	Enterprise license only (NOT consumer/personal)	Drafting, summarization, research using Firm-internal documents	No client PII or PHI without DPA confirmation. Audit logging must be enabled.
[TOOL 2 — e.g., Harvey AI]	[Enterprise plan]	[Permitted use description]	[Any restrictions]
[TOOL 3]	[Version]	[Permitted uses]	[Restrictions]
[Add rows as needed]			

The Approved Tool List is maintained by the AI Governance Owner and updated as tools are evaluated and approved or removed. The current list is always available at [LOCATION/LINK].

4. REQUESTING APPROVAL FOR NEW AI TOOLS

Any Firm personnel who wish to use an AI tool not on the Approved Tool List must submit a request to [AI GOVERNANCE OWNER NAME / EMAIL] before using the tool for Firm business. The request must include the tool name, vendor, intended use, and data types to be entered. The governance owner will evaluate the tool using the Firm's AI Vendor Risk Scorecard and communicate a decision within [10] business days. Use of unapproved tools is prohibited regardless of business purpose.

5. PROHIBITED USES — MANDATORY RESTRICTIONS

The following uses of AI tools are PROHIBITED regardless of the tool or approval status:

5.1 Client Confidential Information: Client names, engagement details, financial information, tax data, legal matter information, or any other client-identifying information may NOT be entered into any AI tool that has not been specifically approved for client data use. This prohibition applies equally to approved tools unless the specific tool is listed as approved for client data in the Approved Tool List. This reflects our obligations under AICPA ET Section 1.700, ABA Model Rule 1.6, and equivalent professional ethics standards applicable to Firm personnel.

5.2 Protected Health Information (PHI): PHI as defined under HIPAA may not be entered into any AI tool unless a HIPAA-compliant Business Associate Agreement (BAA) is in place between the Firm and the AI vendor, and the tool is specifically listed as approved for PHI in the Approved Tool List. Violation of this provision may constitute a HIPAA breach with mandatory notification obligations.

5.3 Social Security Numbers and Government ID Numbers: Social Security Numbers, Employer Identification Numbers, passport numbers, and similar government-issued identifiers may NOT be entered into any AI tool under any circumstances.

5.4 Unapproved Tools: Using any AI tool for Firm business that is not on the Approved Tool List is prohibited. This includes free or personal versions of tools whose enterprise versions are approved.

5.5 Reliance Without Review: AI tool outputs may not be submitted to clients, filed with regulatory bodies, or used as final work product without human review and professional judgment applied by a qualified Firm professional. Personnel remain fully responsible for the accuracy of all work product, regardless of AI assistance.

6. CLIENT DISCLOSURE

The use of AI tools in client engagements must be disclosed to clients as follows:

6.1 Engagement Letter Disclosure: All new client engagement letters entered into after the Effective Date of this policy shall include a disclosure statement describing the Firm's use of AI tools. The standard disclosure language is:

> "[FIRM NAME] uses artificial intelligence tools to support service delivery, including [categories of use — e.g., document review, research, drafting]. All AI-assisted work product is reviewed and approved by a qualified professional before delivery. Client information is handled in accordance with our Privacy Policy and applicable professional ethics obligations. Please contact [CONTACT] if you have questions about our AI practices."

6.2 Client Requests: If a client requests information about whether AI was used in their specific engagement, personnel must respond honestly and completely. Questions about AI use that cannot be answered by the individual should be escalated to [AI GOVERNANCE OWNER] before responding.

7. SECURITY REQUIREMENTS

When using approved AI tools, personnel must observe the following security practices:

- Use only the approved version or plan of the tool (do not use personal/free accounts for Firm business)
- Access AI tools only from Firm-managed devices or devices enrolled in Firm MDM (if BYOD is permitted)
- Never share AI tool credentials with other personnel — use only individual accounts
- Immediately report any suspected AI tool data incidents (unexpected data access, breach notifications, suspicious outputs) to [AI GOVERNANCE OWNER]
- Log out of AI tools when not in active use on shared or unattended devices

8. ENFORCEMENT AND VIOLATIONS

Violations of this policy may result in disciplinary action up to and including termination of employment or engagement. Violations that result in client data exposure, regulatory violations, or breach of professional ethics obligations will be reviewed by firm leadership and may require notification to professional regulatory bodies, affected clients, or regulatory authorities. Personnel who discover a potential violation should report it immediately to [AI GOVERNANCE OWNER] without fear of retaliation.

9. ACKNOWLEDGMENT

All Firm personnel are required to review and acknowledge this policy. Acknowledgment is required upon hire and annually thereafter. By acknowledging this policy, you confirm that you have read, understood, and agree to comply with its terms.

Name (print): _____ Title: _____

Signature: _____ Date: _____

Ready to Get Started?

Axiom Sovereign develops customized AI governance policies for professional services firms — tailored to your industry, regulatory environment, and specific AI tool landscape. calendly.com/cmissimore-6zkc/30min
info@axiomsovereign.com