AI Usage Guidelines Package

CounselWorks Advisory | Prepared with GuardAxis

CounselWorks Advisory receives a high draft risk posture in this Phase 2 demo because the intake indicates internal only AI use with PII, customer content, trade secrets, financial records considerations.

This package is a draft and requires business, security, and legal review before use.

At a Glance

- Included documents: AI Acceptable Use Policy; AI Security and Governance Policy; Employee AI Usage Standard; Third-Party AI Review Checklist.
- Evidence basis: 6 confirmed business inputs and 4 supporting website evidence notes.
- Drafting basis tracked for 8 sections before export.
- Priority risks carried into drafting: 3.

Executive Summary

- Intake answers are treated as the primary source of truth.
- Website evidence is limited to bounded public page review within the requested domain family.
- Policies are presented as editable draft guidelines.

Assumptions and Missing Information

Assumptions

- The website scan in this phase is bounded to public pages within the requested domain family and may be incomplete.
- Framework mappings are provided as high-level drafting references only.

Missing Information

- Public pages do not confirm detailed operational controls for regulated data handling.

Package Snapshot

This draft guidelines package is grounded in 6 business inputs, 4 website evidence notes, and 3 priority risks. Detailed grounding appears in the appendices so the policy language itself stays readable.

Priority Risks

- Sensitive data handling needs explicit AI restrictions (High)

- Source code and proprietary information exposure risk is elevated (High)
- Third-party AI tools need consistent approval and vendor review (Medium)

AI Acceptable Use Policy

AI Acceptable Use Policy

Audience: All staff and contractors | Status: Draft

Draft guidelines only. Review by business, security, and legal stakeholders is required before adoption.

Purpose and scope

CounselWorks Advisory may use approved AI tools to support legitimate business work. These draft guidelines apply to employees and contractors and should be reviewed by business, security, and legal stakeholders before adoption.

Restricted and prohibited uses

AI may support approved work, but it must not be used for prohibited activities such as Do not submit privileged, confidential, or matter-specific client materials into unapproved AI tools.; Do not use AI to make autonomous legal, advisory, engagement, or c...

AI Security and Governance Policy

AI Security & Governance Policy

Audience: Leadership, security, IT, and governance owners | Status: Draft

Draft guidelines only. Review by business, security, and legal stakeholders is required before adoption.

Roles and responsibilities

Business owners, security reviewers, and legal stakeholders should share responsibility for approving AI use cases, reviewing exceptions, and confirming that policy language matches actual operations.

Logging and monitoring

AI-assisted workflows should follow the organization's logging expectations, with additional attention on customer-facing outputs and other high-impact uses. Incident review and exception tracking should be documented in a lightweight, repeatable way.

Employee AI Usage Standard

Employee AI Usage Standard

Audience: Employees and managers | Status: Draft

Draft guidelines only. Review by business, security, and legal stakeholders is required before adoption.

Daily use rules

Employees may use approved AI tools for Internal drafting and research support, Document and matter summarization, Client communication drafts with qualified review, Administrative workflow assistance. Customer-visible or externally shared outputs should st...

Review and verification

AI output must be checked for accuracy, completeness, and business appropriateness before it is relied on. When facts are uncertain or the impact is high, employees should escalate rather than assume the output is correct.

Third-Party AI Review Checklist

Third-Party AI Review Checklist

Audience: Security, procurement, and business owners | Status: Draft

Draft guidelines only. Review by business, security, and legal stakeholders is required before adoption.

Vendor basics

Record the tool name, business owner, intended use case, and whether the tool may affect customers directly. If the use case changes materially, repeat the review.

Data exposure and retention

Review what information the vendor receives, stores, or uses for model improvement. Pay special attention to PII, customer content, trade secrets, financial records, and confirm whether those categories are allowed at all.

Appendix A | Business Inputs

- Organization: CounselWorks Advisory
- Primary website: https://legal-services.guardaxis.io
- AI usage mode: internal only
- Customer-facing AI: Not currently in scope
- Sensitive data types: PII, customer content, trade secrets, financial records
- Current AI tools: ChatGPT, AI features inside productivity tools

Appendix B | Observed Website Evidence

- legal-services.guardaxis.io: CounselWorks Advisory is a sample professional-services practice supporting business clients with legal-adjacent operations and advisory workflows.

  Observed public fact | Source: legal-services.guardaxis.io

- legal-services.guardaxis.io/operations: Teams use AI for internal drafting, document summarization, matter organization, research support, and administrative workflows under qualified review.

  Observed public fact | Source: legal-services.guardaxis.io/operations

- legal-services.guardaxis.io/trust: The sample trust notes emphasize client confidentiality, privilege-aware handling, approved tool use, and review before client-facing language leaves the firm.

  Observed public fact | Source: legal-services.guardaxis.io/trust

- legal-services.guardaxis.io/privacy: The sample privacy notes identify client records, matter context, confidential business documents, financial records, and employee records as sensitive.

  Observed public fact | Source: legal-services.guardaxis.io/privacy

Appendix C | Priority Risks

- Sensitive data handling needs explicit AI restrictions (High)
- Source code and proprietary information exposure risk is elevated (High)
- Third-party AI tools need consistent approval and vendor review (Medium)

Appendix D | Drafting Basis by Section

AI Acceptable Use Policy

Purpose and scope

- Business input: AI usage mode
- Business input: Customer type
- Drafting plan: Purpose and scope

AI Acceptable Use Policy

Restricted and prohibited uses

- Risk driver: Sensitive data handling needs explicit AI restrictions
- Risk driver: Source code and proprietary information exposure risk is elevated
- Risk driver: Third-party AI tools need consistent approval and vendor review
- Drafting plan: Restricted and prohibited uses

AI Security and Governance Policy

Roles and responsibilities

- Business input: New tool approval
- Business input: Vendor review requirement
- Drafting plan: Roles and responsibilities

AI Security and Governance Policy

Logging and monitoring

- Business input: Logging requirement
- Risk driver: customer facing review
- Drafting plan: Logging and monitoring

Employee AI Usage Standard

Daily use rules

- Business input: Internal AI use cases
- Drafting plan: Daily use rules

Employee AI Usage Standard

Review and verification

- Business input: Human review requirement
- Drafting plan: Review and verification

Third-Party AI Review Checklist

Vendor basics

- Business input: Current AI tools
- Drafting plan: Vendor basics

Third-Party AI Review Checklist

Data exposure and retention

- Business input: Sensitive data types
- Drafting plan: Data exposure and retention

Appendix E | Control Mapping

Framework mappings support review and drafting only and should not be treated as proof of compliance.

Review Disclaimer

Draft guidelines only. This material does not establish compliance, certification, or legal sufficiency and must be reviewed by business, security, and legal stakeholders.