# AI Governance & Compliance Policy

CompliGenie Partner

**Prepared for:**

**Acme Legal Associates LLP**

Date: July 30, 2025

# Table of Contents

# Executive Summary

This AI Governance Policy establishes comprehensive guidelines and procedures for the responsible development, deployment, and use of artificial intelligence technologies within Acme Legal Associates LLP. This policy ensures compliance with applicable laws, ethical standards, and industry best practices while maximizing the benefits of AI technology for our clients and stakeholders.

## Key Objectives

- Establish clear governance structures for AI initiatives
- Ensure ethical and responsible AI use across all departments
- Maintain client confidentiality and data privacy
- Comply with all relevant regulations and professional standards
- Promote transparency and accountability in AI decision-making

## Scope

This policy applies to all employees, contractors, and third-party vendors who develop, deploy, or use AI systems on behalf of Acme Legal Associates LLP. It covers all AI technologies including but not limited to machine learning models, natural language processing systems, predictive analytics, and automated decision-making tools.

## Policy Statement

Acme Legal Associates LLP is committed to leveraging AI technology to enhance our legal services while maintaining the highest standards of professional ethics, client confidentiality, and regulatory compliance. We recognize that AI systems must be developed and used in ways that are transparent, accountable, and aligned with our core values of integrity, excellence, and client service.

# AI Usage Guidelines

## 2.1 Approved AI Tools and Applications

The following AI tools have been approved for use within our organization after thorough security and compliance review:

### 2.1.1 Document Analysis and Review

- **Contract Analysis AI:** For reviewing and analyzing legal contracts, identifying key terms, and flagging potential issues
- **Due Diligence Assistant:** For accelerating document review in M&A transactions and corporate matters
- **Legal Research Tools:** Including Westlaw Edge, Lexis+, and CaseText for AI-enhanced legal research

### 2.1.2 Legal Writing and Drafting

- **Brief Assistant:** For initial draft generation of legal briefs and memoranda
- **Contract Drafting Tools:** For creating first drafts of standard agreements
- **Citation Checker:** For verifying legal citations and formatting

### 2.1.3 Client Communication

- **Client Intake Chatbot:** For initial client inquiries and appointment scheduling
- **Email Assistant:** For drafting routine client communications (with mandatory human review)

## 2.2 Prohibited Uses

The following uses of AI are strictly prohibited:

- Making final legal decisions without human attorney review
- Providing legal advice directly to clients without attorney supervision
- Processing sensitive client data through non-approved AI systems
- Using AI to generate court filings without thorough human review and verification

- Sharing confidential client information with AI systems that are not covered by appropriate confidentiality agreements

### 2.3 Human Oversight Requirements

All AI-generated content must be reviewed by a qualified attorney before:

- Submission to any court or regulatory body
- Delivery to clients as legal advice
- Inclusion in any binding legal document
- Publication or external distribution

# Data Protection and Privacy

## 3.1 Client Data Handling

When using AI systems with client data, all personnel must adhere to the following requirements:

### 3.1.1 Data Classification

All client data must be classified according to sensitivity level:

- **Highly Confidential:** Attorney-client privileged communications, litigation strategy, sensitive personal information
- **Confidential:** General client matters, internal memoranda, financial records
- **Internal Use:** Administrative data, scheduling information, general correspondence

### 3.1.2 AI System Requirements

AI systems processing client data must:

- Be hosted in secure, SOC 2 Type II certified environments
- Employ end-to-end encryption for data in transit and at rest
- Maintain detailed audit logs of all data access and processing
- Comply with applicable data residency requirements
- Be covered by appropriate Business Associate Agreements (BAAs) where applicable

## 3.2 Data Retention and Deletion

AI systems must implement the following data retention policies:

- Training data containing client information must be deleted after model training is complete
- AI-generated outputs must be retained according to standard document retention policies
- Audit logs must be retained for a minimum of 7 years
- Client data must be permanently deleted from AI systems upon client request or matter closure

### 3.3 Cross-Border Data Transfers

When AI systems involve cross-border data processing:

- Ensure compliance with GDPR requirements for EU client data
- Implement Standard Contractual Clauses (SCCs) where required
- Obtain explicit client consent for international data transfers
- Maintain records of all cross-border data flows

# Compliance and Regulatory Requirements

## 4.1 Legal and Professional Standards

All AI use must comply with:

### 4.1.1 Bar Association Rules

- **Model Rule 1.1 (Competence):** Attorneys must understand AI capabilities and limitations
- **Model Rule 1.6 (Confidentiality):** Client information must be protected when using AI
- **Model Rule 5.1 (Supervisory Responsibilities):** Partners must ensure proper AI oversight
- **Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistance):** AI systems are treated as nonlawyer assistants

### 4.1.2 Jurisdiction-Specific Requirements

Additional compliance requirements by jurisdiction:

- **California:** Compliance with CCPA and SB 1001 (bot disclosure law)
- **New York:** Adherence to SHIELD Act requirements for data security
- **European Union:** GDPR compliance for all EU client matters
- **Illinois:** Biometric Information Privacy Act (BIPA) compliance

## 4.2 Industry-Specific Regulations

When serving clients in regulated industries, ensure AI compliance with:

- **Healthcare:** HIPAA requirements for protected health information
- **Financial Services:** SOX, Dodd-Frank, and SEC regulations
- **Government Contracts:** FAR and DFARS requirements

## 4.3 Audit and Compliance Monitoring

The firm will conduct:

- Quarterly reviews of AI system compliance
- Annual third-party security assessments
- Regular testing of data protection measures
- Ongoing monitoring of regulatory changes affecting AI use

# Training and Accountability

## 5.1 Mandatory Training Programs

All personnel using AI systems must complete:

### 5.1.1 Initial Training Requirements

- **AI Fundamentals for Legal Professionals** (4 hours)
  - Understanding AI capabilities and limitations
  - Ethical considerations in legal AI use
  - Identifying appropriate use cases
- **Data Security and Privacy in AI** (2 hours)
  - Protecting client confidentiality
  - Secure AI system usage
  - Incident reporting procedures
- **Tool-Specific Training** (varies by tool)
  - Hands-on training for each approved AI tool
  - Best practices and common pitfalls
  - Quality control procedures

### 5.1.2 Ongoing Education

- Annual refresher training (2 hours)
- Updates on new AI tools and features
- Lessons learned from AI incidents
- Regulatory and ethical developments

## 5.2 Roles and Responsibilities

### 5.2.1 AI Governance Committee

Responsible for:

- Approving new AI tools and use cases
- Reviewing compliance reports

- Updating policies and procedures
- Investigating incidents and violations

#### 5.2.2 Department Heads

Responsible for:

- Ensuring team compliance with AI policies
- Identifying training needs
- Reporting AI-related issues
- Implementing quality control measures

#### 5.2.3 Individual Users

Responsible for:

- Completing required training
- Following all usage guidelines
- Reporting concerns or incidents
- Maintaining professional judgment

### 5.3 Violation Consequences

Violations of this policy may result in:

- Mandatory retraining
- Suspension of AI system access
- Formal disciplinary action
- Termination for serious or repeated violations
- Reporting to relevant bar authorities if required

# Implementation Timeline and Next Steps

## 6.1 Implementation Phases

**Phase 1: Foundation (Months 1-2)**

- Establish AI Governance Committee
- Complete initial policy training for all staff
- Audit current AI tool usage
- Implement basic monitoring systems

**Phase 2: Tool Deployment (Months 3-4)**

- Deploy approved AI tools to pilot groups
- Gather feedback and refine processes
- Develop tool-specific guidelines
- Create quality control checklists

**Phase 3: Full Implementation (Months 5-6)**

- Roll out AI tools firm-wide
- Implement comprehensive monitoring
- Establish regular audit schedule
- Launch ongoing training program

## 6.2 Success Metrics

We will measure success through:

- Training completion rates (target: 100% within 60 days)
- AI tool adoption rates (target: 80% of eligible users)
- Efficiency improvements (target: 30% reduction in routine task time)
- Client satisfaction scores (maintain or improve current levels)
- Compliance audit results (target: zero critical findings)

## 6.3 Review and Updates

This policy will be reviewed and updated:

- Quarterly by the AI Governance Committee
- Annually by the Executive Committee
- As needed based on regulatory changes
- Following any significant AI-related incidents

**For questions about this policy or AI usage, contact:**
AI Governance Committee
Email: ai-governance@acmelegal.com
Phone: (555) 123-4567 ext. 890

---