Attach this addendum to the Master Services Agreement or other governing contract between the law firm ("Firm") and the AI vendor ("Vendor").

Law Firm AI Vendor Addendum

1. Purpose. This Addendum governs the protection of confidential, privileged, and sensitive data shared by the Firm with Vendor in connection with Vendor's provision of AI-enabled services. It is intended to ensure compliance with the Firm's legal and ethical obligations to protect client information, uphold confidentiality, and mitigate risks associated with artificial intelligence systems.

2. Definitions

2.1 *Confidential Information* means any data, documents, communications, or other materials transmitted to or accessed by Vendor from or on behalf of the Firm.

2.2 *AI Services* means any system, platform, tool, or process offered by Vendor that uses artificial intelligence, including but not limited to machine learning, natural language processing, and automated inference techniques, to analyze or generate content on the Firm's behalf.

3. Confidentiality Obligations

3.1 Vendor shall treat all Confidential Information as strictly confidential and proprietary to the Firm and/or its clients.

3.2 Vendor shall not access, use, disclose, or retain any Confidential Information except as strictly necessary to provide AI Services under the governing agreement.

3.3 Vendor shall not use Confidential Information for the purpose of training, improving, or fine-tuning AI models unless expressly authorized in writing by the Firm.

3.4 Vendor shall not commingle Confidential Information with data belonging to other Vendor customers, unless expressly authorized in writing by the Firm.

4. Responsible AI Use

4.1 Vendor shall design, test, and operate AI Services in a manner consistent with generally accepted principles of responsible AI use, including fairness, accountability, transparency, and human oversight.

4.2 Vendor shall implement documented procedures to:

4.2.1 Test for and mitigate inappropriate or harmful bias in models and outputs;

4.2.2 Evaluate the accuracy, relevance, and data quality of AI-generated content;

4.2.3 Secure AI systems against prompt injection, jailbreaking, adversarial attacks, and other unauthorized manipulation;

4.2.4 Provide explainability of system functions, outputs, and known limitations, where feasible.

4.3 Vendor shall ensure that all personnel involved in developing or delivering AI Services receive training in responsible AI practices, applicable privacy laws, and ethical obligations relevant to legal-sector clients.

4.4 Vendor shall not knowingly design or deploy AI Services that generate deceptive, misleading, or unauthorized content that may be mistaken for human-generated legal advice or communications.

5. Data Security Requirements

5.1 Vendor shall implement and maintain administrative, technical, and physical safeguards consistent with industry standards for protecting Confidential Information and AI systems.

5.1.1 Security measures shall include, at minimum:

5.1.2 Encryption of Confidential Information in transit and at rest;

5.1.3 Role-based access controls and periodic access reviews;

5.1.4 Secure software development and deployment practices;

5.1.5 Ongoing vulnerability management and penetration testing.

5.2 If Vendor processes any personal data governed by privacy laws (e.g., GDPR, CCPA, HIPAA), it shall do so in compliance with such laws and execute appropriate supplemental agreements (e.g., Data Processing Addendum, Business Associate Agreement) as required.

6. Data Ownership and Return

All Confidential Information, and any output, derivative work, or data generated through AI Services using such Confidential Information, shall remain the exclusive property of the Firm and/or its clients unless expressly authorized in writing by the Firm.

7. Termination and Audit Rights

7.1 In the event of a material breach of this Addendum by Vendor, the Firm may immediately terminate any affected services.

7.2 Upon reasonable notice, the Firm may request documentation, certification, or audit access necessary to verify Vendor's compliance with this Addendum.

8. Conflicts and Priority. In the event of any conflict between this Addendum and the main agreement, this Addendum shall prevail with respect to the protection of Confidential Information in connection with AI Services. In the event of any conflict between this Addendum and any data protection agreement between the Firm and Vendor, the terms most protective of Confidential Information shall prevail.

[Law Firm Name]
By: _____
Name:
Title:
Date:

[Vendor Name]
By: _____
Name:
Title:
Date: