GENERATIVE AI VENDOR VETTING CHECKLIST

Preliminary Questions — Before You Look at Vendors

1. Is there a service that is already in the environment that could do the same or substantially similar task?

   ☐ Yes ☐ No

2. Is this limited to certain users or Firm-wide deployment?

   ☐ Limited Users ☐ Firm-Wide

   Is everyone on board if Firm-wide?

   ☐ Yes ☐ No

3. Will the service require new access, utilize existing access, or require expanded access from existing?

   ☐ New Access ☐ Existing Access ☐ Expanded Access

   What permissions are needed per the AI platform?

   What permissions are needed for users performing the AI task?

Vendor Vetting Checklist

1. Vendor Credibility
   - ☐ Vendor has an established reputation as an AI software provider
   - ☐ Vendor has an established business, leadership team, and legal-industry experience
   - ☐ Vendor can provide references from law firms or legal organizations
   - ☐ Vendor provides documentation of product capabilities and known limitations
   - ☐ Vendor provides documentation of incident response procedures
   - ☐ Vendor has no known data breaches

2. Security and IT Controls
   - ☐ Vendor is SOC 2 Type II certified (or provides equivalent independent security audit)
   - ☐ Data is encrypted in transit and at rest
   - ☐ Multi-factor authentication is available
   - ☐ Vendor has documented breach notification procedures
   - ☐ Vendor provides information on data retention and deletion policies

3. Confidentiality and Data Protection
   - ☐ Client data remains the property of the lawyer or law firm
   - ☐ Vendor does not train models using customer data without consent
   - ☐ Vendor explains whether prompts or uploaded documents are stored
   - ☐ Vendor prevents other users from accessing confidential information
   - ☐ Vendor has sufficient safeguards in place to protect sensitive information from disclosure/leakage
   - ☐ The Lawyer/Firm has sufficient safeguards in place to protect sensitive information from disclosure/leakage

4. Accuracy and Human Oversight
   - ☐ Vendor discloses AI limitations and potential for errors or hallucinations
   - ☐ Product requires or encourages lawyer review of outputs
   - ☐ Vendor provides transparency regarding sources or citations when applicable

5. Ethical and Professional Responsibility Alignment
   - ☐ Vendor acknowledges lawyers' duties of competence, confidentiality, and supervision
   - ☐ Product is designed to assist lawyers, not replace professional judgment
   - ☐ Vendor training materials address responsible AI use in legal practice

6. Contract and Terms of Use
   - ☐ Terms of service protect confidentiality and ownership of client information
   - ☐ Vendor provides reasonable contractual liability protections
   - ☐ Vendor contract includes breach notification and data protection obligations

7. Billing and Fee Transparency
   - ☐ Vendor pricing structure is transparent
   - ☐ Vendor services allow lawyers to comply with ethical billing rules
   - ☐ Pricing does not encourage billing clients for time not actually spent

8. Risk Management Review
   - ☐ Vendor product reviewed internally for malpractice risk exposure
   - ☐ Vendor marketing materials do not imply the tool replaces legal judgment
   - ☐ Vendor agrees to cooperate if claims issues arise involving the tool