Contents

AI Vendor Security Questionnaire for Financial Advisors

Comprehensive Vendor Due Diligence Template

Version 1.0 | March 2026 Provided by AI Secretary

How to Use This Questionnaire

Send this questionnaire to AI vendors during the evaluation process. Their responses will help you assess: - Data security and privacy practices - Compliance with financial services regulations - Business continuity and vendor stability - Alignment with your firm's data retention policies

Rating System: After receiving responses, assign each vendor a risk score: - **Low Risk**: Comprehensive answers, strong security posture, aligns with your policies - **Medium Risk**: Some gaps or concerns, may require contractual safeguards - **High Risk**: Inadequate answers, significant security/compliance concerns, do not proceed

---

Vendor Information

Vendor Name: _____ **Product/Service:** _____
Website: _____ **Primary Contact:** _____
Email: _____ **Phone:** _____

Date Questionnaire Sent: _____ **Date Response Received:** _____ **Evaluated By:** _____

Section 1: Company Information & Stability

1.1 Business Overview

Q1: When was your company founded? - [ ] Response: _____

Q2: How many employees does your company have? - [ ] Response: _____

Q3: How many financial services clients do you serve? - [ ] Response: _____

Q4: Are you a publicly traded company or privately held? - [ ] Response: _____

Q5: Who are your primary investors or parent company (if applicable)? - [ ] Response: _____

1.2 Financial Stability

Q6: Can you provide financial statements or proof of financial stability? - [ ] Response: _____

Q7: Do you carry cyber liability insurance? - [ ] If yes, what is the coverage amount? _____

Q8: Have you received any funding rounds or acquisitions in the past 2 years? - [ ] Response: _____

1.3 Industry Experience

Q9: Do you have experience working with SEC-registered investment advisers? - [ ] Response: _____

Q10: Do you have experience working with FINRA-regulated broker-dealers? - [ ] Response: _____

Q11: Can you provide references from financial services clients? - [ ] Response: _____

Section 2: Data Security & Privacy

2.1 Security Certifications

Q12: What security certifications do you hold? (Check all that apply) - [ ] SOC 2 Type II - [ ] ISO 27001 - [ ] HITRUST - [ ] FedRAMP - [ ] Other: _____

Q13: When was your most recent security audit conducted? - [ ] Date: _____

Q14: Can you provide a copy of your most recent SOC 2 report? - [ ] Response: _____

Q15: Do you undergo regular penetration testing? - [ ] If yes, how frequently? _____ - [ ] Can you share results (redacted)? _____

2.2 Data Encryption

Q16: Is client data encrypted in transit? - [ ] Yes / No - [ ] Encryption standard used: _____

Q17: Is client data encrypted at rest? - [ ] Yes / No - [ ] Encryption standard used: _____

Q18: Where are encryption keys stored? - [ ] Response: _____

Q19: Who has access to decryption keys? - [ ] Response: _____

2.3 Data Storage & Location

Q20: Where is client data stored geographically? - [ ] United States (specify region): _____ - [ ] International (specify country): _____

Q21: What cloud infrastructure provider do you use? - [ ] AWS - [ ] Google Cloud Platform - [ ] Microsoft Azure - [ ] Other: _____ - [ ] None (on-premises): _____

Q22: Is client data stored in multi-tenant environments or single-tenant? - [ ] Response: _____

Q23: Can clients request data to be stored in specific geographic regions? - [ ] Response: _____

2.4 Access Controls

Q24: What authentication methods do you support? - [ ] Username/password - [ ] Multi-factor authentication (MFA) - [ ] Single Sign-On (SSO) - [ ] Biometric authentication - [ ] Other: _____

Q25: Is MFA required for all users? - [ ] Response: _____

Q26: Do you support role-based access control (RBAC)? - [ ] Response: _____

Q27: How often are access permissions reviewed? - [ ] Response: _____

Q28: What is your process for deprovisioning user access when employees leave? - [ ] Response: _____

Section 3: Data Retention & Deletion

3.1 Retention Policies

Q29: How long do you retain client data after it is processed? - [ ] Real-time only (destroyed immediately after processing) - [ ] _____ days - [ ] _____ months - [ ] _____ years - [ ] Indefinitely until client requests deletion - [ ] Other: _____

Q30: Is client data retained in backups after deletion? - [ ] Yes / No - [ ] If yes, for how long? _____

Q31: Can clients configure custom data retention policies? - [ ] Response: _____

3.2 Data Deletion

Q32: Can clients request deletion of their data at any time? - [ ] Response: _____

Q33: How long does it take to fulfill a data deletion request? - [ ] Response: _____

Q34: Do you provide deletion certificates or audit logs confirming data was destroyed? - [ ] Response: _____

Q35: Is deleted data also removed from backups? - [ ] Response: _____

Q36: What is your process for permanent data destruction? - [ ] Response: _____

Section 4: Data Usage & Training

4.1 Model Training

Q37: Do you use customer data to train AI models? - [ ] Yes / No

Q38: If yes, is customer data anonymized before training? - [ ] Response: _____

Q39: Can customers opt out of having their data used for training? - [ ] Response: _____

Q40: Is customer data shared with third parties for model training? - [ ] Response: _____

4.2 Data Sharing

Q41: Do you share customer data with any third-party subprocessors? - [ ] Yes / No

Q42: If yes, please list all subprocessors: - [ ] Response: _____

Q43: Do subprocessors have the same security standards as your company? - [ ] Response: _____

Q44: Can customers request a list of current subprocessors? - [ ] Response: _____

Q45: Do you notify customers before adding new subprocessors? - [ ] Response: _____

Section 5: Compliance & Regulatory Alignment

5.1 Financial Services Regulations

Q46: Does your tool comply with SEC Regulation S-P (Privacy of Consumer Financial Information)? - [ ] Response: _____

Q47: Can your tool support FINRA/SEC recordkeeping requirements (Rule 204-2, Rule 4511)? - [ ] Response: _____

Q48: Can customers export data in a format suitable for regulatory audits? - [ ] Response: _____

Q49: Do you provide audit trails showing data access and modifications? - [ ] Response: _____

5.2 State Privacy Laws

Q50: Does your tool comply with CCPA (California Consumer Privacy Act)? - [ ] Response: _____

Q51: Does your tool comply with other state privacy laws (VCDPA, CTDPA, etc.)? - [ ] Response: _____

Q52: Can you fulfill Data Subject Access Requests (DSARs) on behalf of customers? - [ ] Response: _____

Q53: What is your turnaround time for DSAR fulfillment? - [ ] Response: _____

Section 6: Incident Response & Business Continuity

6.1 Breach Notification

Q54: Have you experienced any data breaches in the past 3 years? - [ ] Yes / No - [ ] If yes, please describe: _____

Q55: What is your breach notification timeline for customers? - [ ] Within 24 hours - [ ] Within 48 hours - [ ] Within 72 hours - [ ] Other: _____

Q56: Who is the primary contact for security incidents? - [ ] Name: _____ - [ ] Email: _____ - [ ] Phone: _____

Q57: Do you have a documented incident response plan? - [ ] Response: _____

6.2 Business Continuity

Q58: What is your uptime SLA? - [ ] 99% | 99.9% | 99.99% | Other: _____

Q59: What is your disaster recovery plan? - [ ] Response: _____

Q60: How frequently do you back up data? - [ ] Response: _____

Q61: What is your Recovery Time Objective (RTO) in the event of an outage? - [ ] Response: _____

Q62: What is your Recovery Point Objective (RPO)? - [ ] Response: _____

6.3 Vendor Stability

Q63: What happens to customer data if your company is acquired? - [ ] Response: _____

Q64: What happens to customer data if your company goes out of business? - [ ] Response: _____

Q65: Do you have a data transition plan for customers who wish to migrate to another vendor? - [ ] Response: _____

Q66: Can customers export all their data at any time? - [ ] Response: _____

Section 7: Terms of Service & Contractual

7.1 Service Agreement

Q67: Can we review your standard service agreement before signing? - [ ] Response: _____

Q68: Are you willing to negotiate custom terms for security and data retention? - [ ] Response: _____

Q69: Do you offer Business Associate Agreements (BAAs) for HIPAA compliance? - [ ] Response: _____

Q70: What is your contract termination policy? - [ ] Response: _____

7.2 Liability & Indemnification

Q71: What is the liability cap in your standard agreement? - [ ] Response: _____

Q72: Do you provide indemnification for data breaches caused by your negligence? - [ ] Response: _____

Q73: Do you have errors & omissions (E&O) insurance? - [ ] Response: _____

Q74: Can you provide proof of insurance coverage? - [ ] Response: _____

7.3 Changes to Terms

Q75: Can you change terms of service unilaterally? - [ ] Response: _____

Q76: How much advance notice do you provide before terms changes? - [ ] Response: _____

Q77: Can customers terminate without penalty if terms change materially? - [ ] Response: _____

Section 8: AI-Specific Questions

8.1 Model Transparency

Q78: What AI models or technologies power your product? - [ ] Response: _____

Q79: Are AI models trained on proprietary data or public datasets? - [ ] Response: _____

Q80: Can you explain how your AI processes client data? - [ ] Response: _____

Q81: Do you provide transparency into AI decision-making (explainability)? - [ ] Response: _____

8.2 Accuracy & Reliability

Q82: What is the accuracy rate of your AI outputs? - [ ] Response: _____

Q83: How do you handle AI errors or "hallucinations"? - [ ] Response: _____

Q84: Do you recommend human review of AI-generated outputs? - [ ] Response: _____

Q85: Can customers report inaccuracies or provide feedback to improve the model? - [ ] Response: _____

8.3 AI Safety & Ethics

Q86: Do you have an AI ethics policy? - [ ] Response: _____

Q87: How do you prevent bias in AI models? - [ ] Response: _____

Q88: Do you conduct fairness audits on AI models? - [ ] Response: _____

Q89: Are there any known limitations or risks of your AI system? - [ ] Response: _____

Section 9: Support & Training

9.1 Customer Support

Q90: What support channels do you offer? - [ ] Email - [ ] Phone - [ ] Live chat - [ ] Dedicated account manager - [ ] Other: _____

Q91: What are your support hours? - [ ] Response: _____

Q92: What is your average response time for support tickets? - [ ] Response: _____

Q93: Do you offer 24/7 emergency support for critical incidents? - [ ] Response: _____

9.2 Training & Onboarding

Q94: Do you provide onboarding and training for new customers? - [ ] Response: _____

Q95: What training materials are available? - [ ] Documentation - [ ] Video tutorials - [ ] Live training sessions - [ ] Certification programs - [ ] Other: _____

Q96: Do you provide compliance training or documentation to help customers meet regulatory requirements? - [ ] Response: _____

Section 10: Pricing & Billing

10.1 Cost Structure

Q97: What is your pricing model? - [ ] Per user/seat - [ ] Per transaction - [ ] Flat monthly fee - [ ] Usage-based (tokens, API calls, etc.) - [ ] Other: _____

Q98: Are there any hidden fees or additional costs? - [ ] Response: _____

Q99: Do you offer discounts for annual commitments? - [ ] Response: _____

Q100: What is your cancellation policy and are there penalties for early termination? - [ ] Response: _____

Evaluation Summary

Vendor Risk Assessment

Based on responses, assign an overall risk rating:

- ☐ **Low Risk** — Proceed with confidence
- ☐ **Medium Risk** — Proceed with contractual safeguards
- ☐ **High Risk** — Do not proceed

Key Strengths

1. _____
2. _____
3. _____

Key Concerns

1. _____
2. _____
3. _____

Required Actions Before Approval

- ☐ _____
- ☐ _____
- ☐ _____

Compliance Officer Approval

- ☐ **Approved** — Vendor meets our standards
- ☐ **Approved with Conditions** — Specify: _____
- ☐ **Denied** — Does not meet standards

Reviewed By: _____ **Title:** _____
Signature: _____ **Date:** _____

Appendix: Red Flags

Do NOT proceed if vendor: - Cannot or will not answer security questions - Does not hold SOC 2 or equivalent certification - Stores data indefinitely without deletion options - Uses customer data to train models without opt-out - Has experienced multiple breaches in past 3 years - Cannot provide breach notification within 48 hours - Stores data internationally without transparency - Does not encrypt data in transit and at rest - Claims proprietary/confidential on basic security questions - Has unstable financial situation or unclear ownership

---

Next Steps

After receiving completed questionnaire:

1. **Review Responses**: Evaluate completeness and adequacy
2. **Request Follow-Up**: Ask for clarification on any vague answers
3. **Request Documentation**: Ask for SOC 2 reports, insurance certificates, etc.
4. **Conduct Reference Checks**: Contact financial services clients using the vendor
5. **Negotiate Contract**: Address any concerns via contractual safeguards
6. **Get Final Approval**: CCO or senior leadership sign-off
7. **Document Decision**: Maintain questionnaire and evaluation in compliance files

---

This questionnaire is provided for informational purposes only and does not constitute legal or compliance advice. Firms should consult with legal counsel and compliance professionals when evaluating vendors.

Provided by AI Secretary aisecretary.tech The only audit-ready AI meeting assistant with Zero-Retention Architecture

See how we answer these questions: https://aisecretary.tech/security

---

Questionnaire Version 1.0 | March 2026