

AI WSP Instructions and Elections

A reusable template for documenting your Firm's AI permissions, oversight and vendor review.

Complete the template

1. Download this PDF and open it in Adobe Acrobat Reader or Acrobat. Complete the two-page Election Form and save a Firm-specific copy.
2. Enter Firm and officer details once. Those entries apply throughout the policy. Choose the authorized level of use, permitted activities and information restrictions.
3. Review related WSP chapters and vendor procedures before adoption. Elections establish scope; they do not replace required tool reviews, approvals or controls.

Use a referenced attachment for longer answers. Typed approvals are approval records, not certificate-based digital signatures.

Need a customized plan

Contact Compliance.Network for a plan tailored to your Firm's AI uses, vendor relationships and supervisory procedures.

Talk to us at compliance.network/contact.html

PROFESSIONAL NOTICE

Compliance.Network is not a law firm and does not provide legal advice or legal representation. This template is for informational purposes and should be reviewed by qualified legal counsel before use.

[Privacy Policy](#)

[AI Transparency](#)

Adoption and implementation

Use this template to establish and document the Firm's AI policy, vendor reviews, approvals, and supervision. Complete the applicable records and review related procedures before adoption.

Assign responsibility. Identify the CEO, CCO, Designated Principal, or Designee responsible for administering the procedures. Record the selected officer and title, any delegation, and approval dates. In the chapter, this person is referred to as the Responsible Officer.

Complete the elections before adoption. Identify the responsible person, select one level of AI use, and complete the permitted activities and information restrictions. Unselected activities and information categories remain prohibited. Sign and date the Election Form. The approved form is incorporated into the WSP chapter; the Firm does not need to rewrite the chapter to reflect its elections.

Review related WSP chapters. Adopting this AI chapter alone may not be sufficient. Review other WSP chapters and revise them where the Firm's AI use or vendor practices affect existing requirements. Areas may include third-party vendor oversight, information security and privacy, books and records, communications and advertising, social media, client analysis, product due diligence or structuring, employee training, and incident response. Document affected chapters, revisions, approvals, and effective dates; record when no revision is needed and why.

Update vendor procedures. Review actual products, subscriptions, AI features, information flows, and settings. Document service-specific controls in the relevant vendor procedure or addendum. Published policies and terms may be sufficient; request targeted clarification only for material gaps. No vendor is preapproved by this package.

Maintain the approved elections. Retain the current and superseded Election Forms with compliance records. Keep tool approvals, vendor reviews, restrictions, and supporting evidence in the Firm's designated records repository. Communicate the elections to affected personnel. Review at least annually and before implementing changes.

AI Risk Disclosure

AI tools and vendor AI processing can create risks for the Firm, its personnel and clients. Approval of a tool or activity does not guarantee accuracy, confidentiality, security or compliance. Consider these risks before using AI or relying on its output.

Cybersecurity and unauthorized access

AI accounts, connected systems and vendors may be hacked or compromised. Stolen credentials, excessive permissions or insecure integrations can expose information or allow unauthorized actions.

Malicious inputs and instructions

Documents, messages, websites or other inputs may contain instructions intended to manipulate an AI tool. A connected tool may disclose information, produce misleading results or perform unintended actions if those instructions are followed.

Confidentiality and privacy

Information entered into a tool may be retained, shared, accessed by subcontractors or used for model training under the applicable terms and settings. Sensitive information can also appear in generated outputs or be disclosed to unintended recipients.

Inaccurate or misleading output

AI can invent facts, citations or calculations; omit important information; use outdated sources; or produce plausible but incorrect conclusions. Outputs may vary even when similar questions are asked.

Bias and inappropriate content

Outputs may reflect biased assumptions, treat people inconsistently or include unsuitable content. Human review remains necessary for the intended audience and use.

Intellectual property and records

Inputs or outputs may raise questions about ownership, licensing, confidentiality or permitted reuse. Tools may not preserve the records, sources or review evidence the Firm needs.

Vendor changes and service failures

Vendors can change models, terms, settings or subcontractors. Outages, unavailable records or unexpected behavior can interrupt work or undermine previously reviewed controls.

Automation and overreliance

AI agents and integrations can repeat errors, send communications, alter records or initiate actions beyond the intended scope. Reliance on AI can weaken independent judgment and allow errors to spread before detection.

Follow approved limits, verify material outputs, protect credentials, restrict access and promptly report suspected compromise, exposure, unauthorized use or other problems to the Responsible Officer. Apply the Firm's incident response and corrective action procedures. Controls reduce risk; they do not eliminate it.

Firm AI Use Elections

Complete this page and the following page. The approved Election Form is incorporated into the WSP chapter. Elections define permitted scope; required tool, vendor and implementation reviews and approvals still apply.

Firm legal name	Election version and effective date

Responsible Officer role

Select

Responsible Officer name	Delegation or authority reference, if applicable

Authorized level of AI use - select one

Select

Level 1: leave activities and information categories unselected; disable controllable features and document the treatment of vendor AI processing. Level 2: selected activities must occur through approved embedded features or vendor processing. Level 3: selected activities may also use approved standalone tools. Resolve inconsistent or incomplete elections before implementation.

Permitted activities - check all that apply

- ☐ Internal administration and document assistance
- ☐ Research and summarization
- ☐ Coding and technology support
- ☐ Meeting recording and transcription
- ☐ Client analysis or recommendations
- ☐ Product due diligence or structuring
- ☐ Marketing and advertising
- ☐ Social media
- ☐ Client-facing AI interactions
- ☐ Agents or automated decisions and actions

Other activity and specific scope, or None

Restrictions and Approval

Continuation of the Election Form. Unselected information categories remain prohibited. For Level 1, leave all information categories unselected. Approval must cover both the service and the information processed.

Information permitted for approved processing

- ☐ Public information
- ☐ Internal nonconfidential information
- ☐ Proprietary or confidential Firm information
- ☐ Confidential client information
- ☐ Personal information

Additional information exclusions or limits, or None

Every new tool, vendor AI use, feature, integration or implementation requires documented review and written approval by the Responsible Officer before activation. Approval may cover defined users and recurring activities within its documented scope; approval for each routine task is not required.

Approved tool register or approval records location

Additional reviewers or approvals required, or None

Activity limits, human review, automation limits and procedure references

Approval confirms the Firm's intended scope. Required reviews, controls, communications and affected procedure revisions must be completed before use begins. Changes require an approved revised Election Form and review of affected procedures before implementation.

Responsible Officer approval - type Approved

Approval date

Personnel notification and evidence reference

Next annual review date

Prior election version superseded, or Initial adoption

Artificial Intelligence WSP Chapter

The adopting Firm, Responsible Officer and effective elections are identified in the completed Election Form. Retain that form with this chapter.

For this chapter, “Firm” means the adopting entity identified above. The “Responsible Officer” is the CEO, CCO, Designated Principal, or Designee identified in the Firm’s current approved AI Use Election Form.

Policy

The Firm’s completed and approved AI Use Election Form is incorporated into this policy by reference and establishes the Firm’s authorized level of artificial intelligence (“AI”) use, permitted activities, information restrictions, designated supervisory responsibility, and approval requirements.

Only uses expressly permitted by the current approved Election Form may be considered for implementation under these procedures. An election does not, by itself, approve a particular tool, vendor, or implementation. Required reviews, written approvals, and controls must be completed before use begins. Uses not expressly permitted are prohibited. If no Election Form has been approved, no AI use is authorized; identified embedded features and vendor processing must be reviewed and addressed under these procedures.

The Firm may use platforms with embedded AI features, including Microsoft products, and vendors may use AI in providing services. Feature availability, vendor default settings, or vendor AI use does not itself authorize use. The Responsible Officer will approve and date the Election Form, communicate permissions and restrictions, and retain current and superseded versions. Changes require documented approval and review of affected supervisory and vendor procedures before implementation.

The AI Risk Disclosure in this document forms part of this policy. Personnel must follow approved safeguards and promptly report suspected compromise, information exposure, inaccurate material outputs or unintended actions to the Responsible Officer.

Responsibility

The Responsible Officer administers this policy, reviews proposed AI uses, evaluates vendor AI practices, and oversees approved limitations. Tasks may be assigned to management, technology personnel, or service providers, with review and approval retained by the Responsible Officer. Associated persons must comply with restrictions and promptly report known or suspected unauthorized AI use to that officer.

Supervisory Procedures

Identification and review

At least annually, and upon learning of a material change, the Responsible Officer will review identified AI features in the Firm’s technology platforms and known AI uses by service providers. The review will consider the service, actual subscription and configuration, information accessed, users, and whether default settings or available features conflict with this policy. The Firm will maintain an inventory and document required configuration changes, restrictions, and follow-up.

Artificial Intelligence WSP Chapter

Vendor review and evidence

Before engaging a new vendor known to use AI for the Firm, or permitting a material new AI use by an existing vendor, the Responsible Officer will evaluate the proposed service and information involved. Existing vendors will be included in the annual review. Review may rely on published AI use policies, privacy notices, service terms, data protection terms, security materials, contractual commitments, and documented configuration settings relevant to the actual product and subscription. A vendor questionnaire is not required for every vendor. Published materials may be sufficient for a provider such as Microsoft if they address the Firm's actual use and material concerns. Vendor size or reputation alone is not sufficient.

Matters evaluated

The review will address, as applicable: the purpose and scope of AI use; information accessed or processed; use of inputs and outputs for model training or other secondary purposes; collection, sharing, retention and deletion; access by subcontractors and AI providers; security and incident notification; reliability and human oversight; available restrictions or opt-outs; and notice of material changes. The reviewer will assess consistency with the Firm's confidentiality obligations and intended service.

Follow-up and determination

If material questions remain, the Responsible Officer will seek targeted clarification, request a questionnaire where useful, obtain additional documentation, or impose restrictions. The determination will state whether the vendor AI use is acceptable, acceptable with restrictions, unacceptable, or pending further information, with supporting reasons. An unanswered questionnaire does not automatically require rejection, but an unresolved material concern cannot be treated as approval. Pending review, affected new processing will not begin; existing affected processing will be restricted, suspended, or otherwise addressed as documented by the Responsible Officer.

Vendor specific procedures

Approved features, configurations, access permissions, information restrictions, required human review, responsible personnel, review frequency, and evidence location will be documented in the affected vendor's existing procedures or a vendor-specific addendum. This chapter establishes the general framework; it does not replace vendor-specific operating and supervisory procedures. A vendor's AI use does not authorize an activity prohibited by this chapter.

Approval of proposed uses

Before enabling a tool, feature, integration, or business use, the requesting person will submit its purpose, information, users, and vendor details to the Responsible Officer. That officer will confirm that the proposed use fits the current approved elections and evaluate confidentiality, security, vendor practices, reliability, human review, supervision, and record retention. Written approval will identify the permitted purpose, users and information, conditions, and supporting procedure references. A use outside the elections requires an approved Election Form revision before implementation. An election cannot waive a required review or control.

Artificial Intelligence WSP Chapter

Controls for approved activities

Before activation, the Responsible Officer will document controls suited to the use, information involved, and potential effect on clients or the Firm. Controls will identify a supervisor, review steps, records, and restrictions. For analysis, research, product work, or client-related outputs, specify verification and qualified human review before reliance. For marketing, social media, or other communications, apply the Firm's applicable content review, approval, and retention procedures. For recording or transcription, address notices or consent where applicable, access, retention, and deletion. For coding, integrations, agents, or automated actions, define access permissions, testing, human authorization, operating limits, and a means to stop or restrict activity. Client-facing AI must have an approved scope, oversight, escalation path, and applicable disclosures. These activities may begin only after the relevant controls and affected WSP or vendor procedures are in place.

Protection of information

Associated persons may not submit confidential client information, personal information, or proprietary Firm information to AI tools, or provide it for vendor AI processing, without written approval covering the tool or service and information involved. Associated persons may not independently activate AI features, integrations, or subscriptions for Firm business without approval from the Responsible Officer.

Monitoring and exceptions

At least annually, the Responsible Officer will review compliance through personnel inquiries and available settings, vendor disclosures, access records, or other relevant evidence. Material changes to AI use, privacy terms, services, information processed, or configurations will prompt reassessment. Unauthorized use will be investigated and corrective action documented, including restrictions, response to information exposure, training, or management escalation as appropriate.

Communication

The Responsible Officer will communicate this policy and changes to approved uses or restrictions to affected personnel. Relevant notices and acknowledgments will be retained.

Documentation

The Responsible Officer will retain inventories, review evidence and policy versions, vendor inquiries and responses, determinations and rationale, approvals and restrictions, vendor procedure updates, supervisory reviews, employee communications, exceptions, and corrective actions in the Firm's designated compliance records repository under its record retention procedures. Evidence records will identify the product, relevant terms or settings, source, version or access date, reviewer, and review date.