This AI Acceptable Use Policy is a generalized template provided by Andersen Consulting, LLC. It should not be used as is. Careful consideration must be taken to customize AI Acceptable Use Policies to cover your operational reality.

Name: [Policy Reference] – Artificial Intelligence Responsible Use Policy

Date: [Date]

PURPOSE

The Firm is committed to the responsible, ethical, and secure use of artificial intelligence ("AI") technologies in the delivery of professional services and in internal Firm operations. This policy establishes requirements governing the use of AI, including generative AI and AI agents, to protect confidential family and Firm information, comply with applicable laws and professional standards, and ensure that human judgment, professional skepticism, and accountability remain central to all Firm work product.

SCOPE

This policy applies to all principals, family members, executives, employees, contractors, and third parties acting on behalf of the Firm and its affiliates ("Firm Personnel"). Oversight of AI usage is shared across the Firm. The Chief Operating Officer is responsible for technical governance, including platform approval, security controls, data retention, and integration architecture. The General Counsel, the Chief Compliance Officer, and the Chief Investment Officer are responsible for professional, regulatory, and ethical oversight of AI-assisted work.

POLICY

AI Risk Classification Framework

The Firm classifies AI use cases into risk tiers based on their potential impact on family outcomes, regulatory compliance, and financial reporting: (a) **Low Risk** – administrative support, formatting, and internal drafting with no impact on the family; (b) **Moderate Risk** – research, summarization, and internal analysis; (c) **High Risk** – investment advice, tax positions, financial modeling, legal interpretations, or deliverables relied upon by the family; and (d) **Prohibited Use Cases** – any use that violates confidentiality, law, or this policy. Higher-risk use cases require enhanced review, documentation, approval, and monitoring. Firm Personnel must ensure that AI usage aligns with the designated risk tier and applicable controls prior to use.

Confidential Family and Firm Data

It is never acceptable to input, upload, prompt, record, or otherwise expose confidential family data or confidential Firm data to any third-party website, AI tool, application, browser extension, or platform that has not been explicitly approved by the Chief Operating Officer for the transmission and processing of such data. See Appendix A: Approved AI Tools and Websites.

The Firm maintains enterprise licenses for certain AI platforms that are centrally configured to prevent unintentional data retention and model training. Only Firm Personnel with authorized access to these enterprise platforms may input confidential family or Firm data into AI tools. Firm Personnel may use

public, free, or personal subscription AI tools solely for purposes that do not involve confidential family or Firm data. Information must be fully anonymized, and if the identity of a family member, individual, or matter could reasonably be inferred, the information is deemed confidential and may not be used. Use of personal API keys or unauthorized integrations for Firm business purposes is strictly prohibited. The Firm reserves the right to monitor and restrict access to unauthorized AI tools through technical controls, including browser-based and network controls.

Confidential family and Firm data are protected by law. A breach of confidential family data may result in legal action, penalties, and/or criminal liability to the Firm or the personnel responsible for the breach. Any unauthorized disclosure of confidential family or Firm data must be reported immediately in accordance with the Firm's Security Incidents Response Policy.

For the purposes of this policy, the following definitions apply:

Confidential Family Data includes all personally identifiable information (PII) including names, initials, social security numbers, addresses, telephone numbers, email addresses, information contained on driver's licenses, passports, or other forms of government ID. It includes financial, tax, legal, and transactional information, confidential communications, and contextual information that could reasonably identify a family member.

Confidential Firm Data includes all non-public information relating to the Firm, including financial information, strategies, family and beneficiary lists, employee and contractor information, internal communications, and governance documents.

AI Training, Retention, and Data Vault Controls

The use of confidential family data, confidential Firm data, or Firm work product to train open or public AI models is strictly prohibited.

To reduce risk when working with sensitive information, the Firm maintains a secure Data Vault architecture that tokenizes PII and other sensitive data. Original data is stored in encrypted form, and tokens are used in downstream analytics, automation, and approved AI-enabled workflows. Access to original data and detokenization functions is strictly controlled, logged, and auditable.

Direct PII may never be entered into AI tools outside of approved enterprise platforms or the Data Vault environment. All AI interactions involving Firm or family-related work must be capable of audit and reconstruction. Where AI materially contributes to work product, Firm Personnel must retain sufficient records of prompts used, tools and model versions utilized, and outputs generated to support audit, regulatory review, or internal quality assurance.

Third-Party AI Usage

The Firm may engage third-party vendors, service providers, or contractors that utilize AI in their internal processes or in the delivery of services to the Firm. Such third parties must be evaluated through the Firm's vendor risk management processes, including assessment of data security, confidentiality controls, AI governance practices, and compliance with applicable laws and contractual obligations.

Where appropriate, the Firm may require contractual representations, audit rights, or independent assurance reports regarding a third party's AI controls and data handling practices.

Third-party AI providers must include a contractual obligation to notify the Firm of any security event or data breach in accordance with the Firm's Security Incidents Response Policy. Third-party AI providers must also be evaluated for intellectual property risks, including the potential use of training data that may infringe on third-party rights, and for compliance with applicable data localization and cross-border data transfer regulations.

Family Disclosure in Engagement Agreements

Where AI tools are used in the delivery of services, engagement letters or service agreements should include disclosure language advising the family that:

> *In the performance of services, the Firm may use artificial intelligence through tools that do not require the disclosure of personally identifiable information, and do not train on family data. All deliverables remain subject to human review and professional judgment.*

The scope and nature of AI usage should be consistent with applicable professional standards and contractual obligations.

Use of Generative AI Content

Generative AI may be used to assist with research, drafting, analysis, and workflow efficiency; however, such tools may produce inaccurate, incomplete, or fabricated information. Firm Personnel must independently verify all facts, citations, statutes, regulations, and professional guidance prior to use. AI-generated output must never be relied upon as the sole source of technical, legal, tax, or accounting advice.

AI-generated outputs must be evaluated for accuracy, completeness, bias, and logical consistency. Firm Personnel must ensure that outputs do not contain discriminatory assumptions, unsupported conclusions, or fabricated authorities. Where AI is used in high-risk use cases, personnel must be able to explain how the AI output was derived and how it was validated prior to reliance. Documentation of the review of AI-generated content should be maintained as part of work papers or engagement records, consistent with applicable professional standards.

AI-Generated Calculations and Spreadsheets

Special care must be exercised when AI tools are used to generate calculations, models, spreadsheets, or Excel-based analyses. Any AI-generated calculations or formulas must be independently validated, recalculated, and reviewed by qualified Firm Personnel prior to use. Spreadsheets or models created or modified using AI must be documented to identify the nature of AI assistance and the validation steps performed.

Similar controls apply to AI-generated code, scripts, or automation. All AI-generated code must be reviewed for security vulnerabilities, logical accuracy, and compliance with applicable licensing requirements prior to use. AI-generated applications must be approved by the Chief Operating Officer, the General Counsel, and the Chief Compliance Officer prior to release for operational use or use with family data.

AI Agents and Automated Systems

AI agents are systems capable of autonomous or semi-autonomous execution of tasks or workflows. AI agents may not be deployed or used without formal approval from the Chief Operating Officer, the General Counsel, and the Chief Compliance Officer.

The Chief Operating Officer will maintain a catalogue of approved AI agents that records the owner of each agent, the data that the agent can access, the Firm Personnel with permission to use the agent, and its intended purpose or function. All AI agents must maintain detailed activity logs sufficient to support monitoring, audit, and investigation. Agents must include mechanisms for human override or immediate shutdown ("kill switch") in the event of unintended behavior. AI agents must be periodically reviewed to confirm continued alignment with their approved purpose, data access permissions, and risk classification.

AI agents may not make final decisions affecting investment advice, legal conclusions, tax positions, or financial reporting, nor may they communicate directly with the family without human review. All outputs remain the responsibility of supervising Firm Personnel.

AI Notetaking and Recordings

AI notetaking or recording tools may not be used for meetings involving confidential family or Firm data. If a family member insists on use, Firm Personnel must disclose Firm policy concerns and obtain unanimous consent. If AI notetaking or a recording is made through the Firm's approved enterprise meeting platform, a popup window that requires click-through consent from all participants satisfies this policy's requirements.

If a meeting is initiated on any other platform, Firm Personnel must advise all participants that the Firm has not evaluated the security of the platform and must secure consent from all participants. If any party objects, the recording must cease or Firm Personnel must decline the meeting.

AI Governance, Monitoring, and Change Management

To ensure consistent, controlled, and auditable use of artificial intelligence across the Firm, the Firm maintains governance processes addressing approval, monitoring, model changes, and operational resilience.

Approval and Risk-Based Authorization

AI use cases must be reviewed and approved in accordance with their risk classification:

1. Low Risk use cases may be utilized without formal pre-approval, provided they comply with this policy.
2. Moderate Risk use cases may require department-level or engagement-level oversight as determined by the Chief Operating Officer.
3. High Risk use cases, including those involving investment advice, financial reporting, tax positions, or other material deliverables, must be approved in advance by appropriate leadership, which may include the Chief Operating Officer, the General Counsel, and/or the Chief Compliance Officer.

Approval records must be maintained and made available for audit or review upon request.

Monitoring and Governance Oversight

The Firm reserves the right to monitor the use of AI tools to ensure compliance with this policy and applicable law.

Monitoring may include:

- Usage patterns of approved AI tools
- Access to and attempted use of unauthorized AI tools
- High-risk use case activity and outputs
- AI-related incidents or policy violations

The Firm may establish governance committees or oversight functions responsible for periodic review of AI usage, emerging risks, and compliance trends, including reporting to Firm leadership and the family where appropriate.

Model and Tool Change Management

Approved AI tools and underlying models are subject to ongoing evaluation. Material changes to AI tools, including significant updates to model capabilities, behavior, data handling practices, or vendor terms, must trigger re-evaluation of their suitability for approved use cases.

Where appropriate, the Firm may require:

- Revalidation of outputs for high-risk use cases
- Updated documentation or approvals
- Temporary suspension of use pending review

Firm Personnel must use only currently approved tools and configurations and may not rely on prior approvals if a tool or model has materially changed.

Data Jurisdiction and Re-Identification Risk

AI tools must be used in a manner consistent with applicable data protection, privacy, and data localization laws. Firm Personnel may not use AI tools in a way that results in the unauthorized transfer of data across jurisdictions or into environments that do not meet Firm requirements.

Information that has been anonymized or tokenized must not be used if there is a reasonable possibility that the data could be re-identified, whether alone or in combination with other available information.

Business Continuity and Operational Resilience

AI tools are intended to enhance, but not replace, professional processes. Firm Personnel must ensure that critical workflows, family deliverables, and Firm operations do not depend solely on the availability of AI tools.

Appropriate fallback procedures must be maintained to allow continued operation in the event of AI tool unavailability, vendor disruption, or access restrictions.

Oversight and Documentation Standards

Any AI-generated content incorporated into family deliverables or Firm work product must be subject to a level of review and documentation commensurate with the risk classification of the use case. Documentation must, where applicable, include: (a) a description of how AI was used; (b) identification of tools and models utilized; (c) validation steps performed, including independent verification of facts, citations, and calculations; and (d) evidence of human review and approval. The Firm may issue practice aids providing further guidance on documentation standards and oversight expectations by risk level and function.

Responsible Use

Firm Personnel are prohibited from using AI tools to generate false, misleading, discriminatory, or offensive content, or from circumventing safeguards designed to protect data and confidentiality.

Intellectual Property and Data Rights

Firm Personnel must ensure that AI-generated content does not infringe upon third-party intellectual property rights. AI tools that rely on unknown or unverified training data sources must not be used for family deliverables without appropriate review. All work product generated using AI in the course of employment remains the property of the Firm, subject to applicable agreements.

Training and Certification

All Firm Personnel must complete mandatory AI responsible use training prior to accessing approved enterprise AI tools and must complete periodic refresher training thereafter. Additional role-based training may be required for personnel engaged in high-risk AI use cases as determined by the Chief Operating Officer.

Prohibited Uses of AI

The following activities are strictly prohibited: (a) inputting confidential or identifiable family data into unapproved AI tools; (b) relying on AI-generated outputs as the sole basis for professional advice without independent human review; (c) using AI to generate misleading, deceptive, or fraudulent content; (d) circumventing Firm security, monitoring, or approval controls; and (e) using AI to impersonate family members, regulators, or other third parties.

Compliance and Enforcement

Misuse of AI technologies creates significant risks to the Firm. The Firm reserves the right to monitor AI usage consistent with applicable law. Violations of this policy may result in disciplinary action, up to and including termination.

AI-related incidents, including unauthorized data exposure, improper use of AI tools, or reliance on materially incorrect AI-generated outputs, must be reported in accordance with the Firm’s Security Incidents Response Policy. Such incidents may be subject to enhanced review due to the unique risks associated with AI systems.

This policy will be reviewed periodically and updated as laws, regulations, and professional standards evolve.

ATTACHMENT(S): Appendix A – Approved AI Tools and Websites

Version	Date	Description of Changes	Chief Operating Officer Approval	General Counsel Approval	Chief Investment Officer Approval	Principal Approval
1.0	[Date]	Initial Release	[Chief Operating Officer]	[General Counsel]	[Chief Investment Officer]	[Principal]

Artificial Intelligence Responsible Use Policy
Appendix A: Approved AI Tools and Websites

1. [Approved enterprise generative AI platform – firmwide license]
2. [Approved enterprise generative AI platform – limited pilot license]
3. [Approved enterprise productivity AI assistant – for personnel with Firm-issued licenses]