

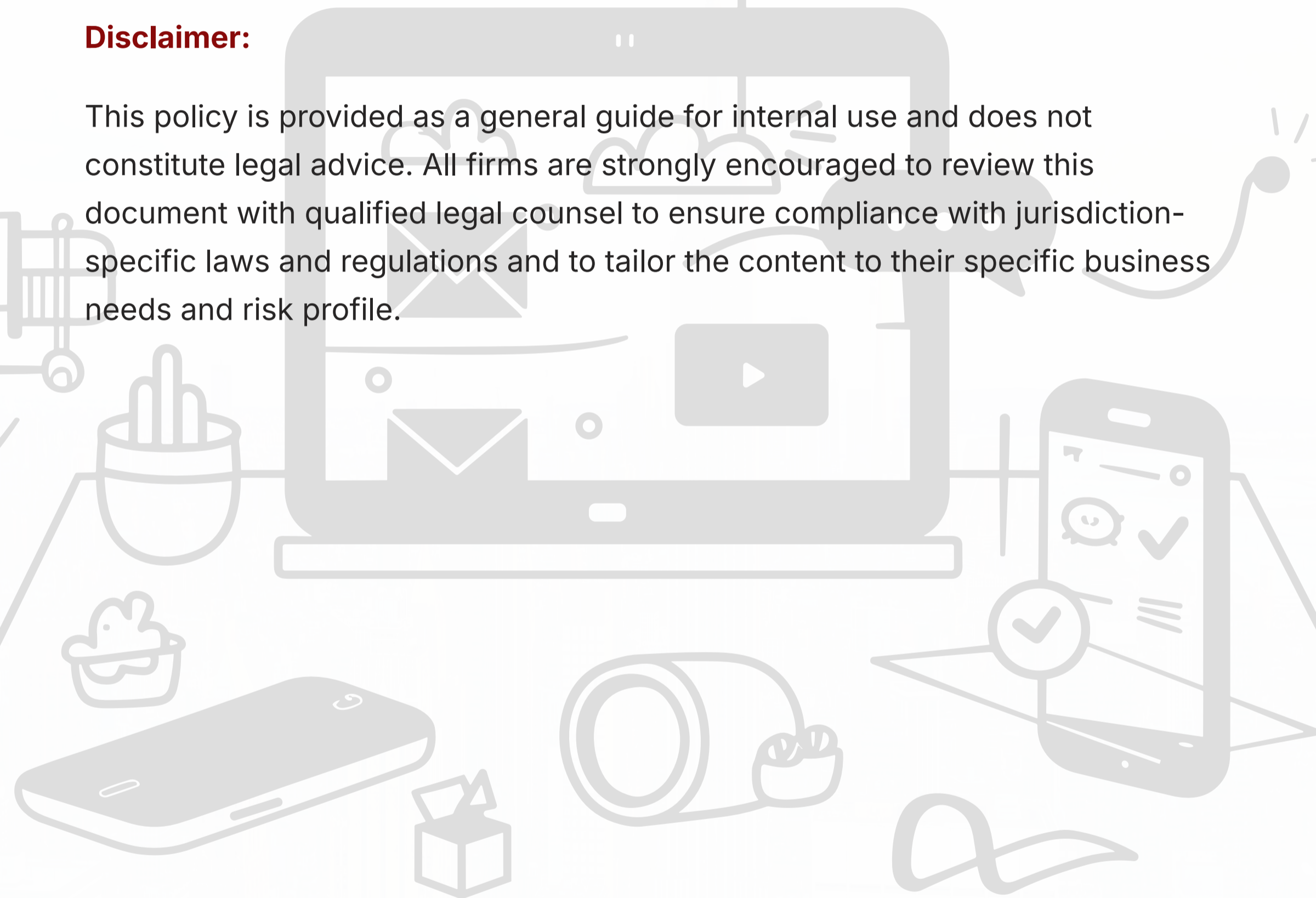
AI Policy for M&A Advisory Firms

This policy establishes guidelines for the responsible and secure use of Artificial Intelligence (AI) tools within our M&A advisory firm. It is designed to enhance operational efficiency, ensure compliance with applicable regulations, protect client confidentiality, and maintain our reputation for trusted, high-integrity advisory services.

 **by Carl de Prado**

Disclaimer:

This policy is provided as a general guide for internal use and does not constitute legal advice. All firms are strongly encouraged to review this document with qualified legal counsel to ensure compliance with jurisdiction-specific laws and regulations and to tailor the content to their specific business needs and risk profile.



Scope and Acceptable Use

This policy applies to all employees, consultants, contractors, and partners who access or utilize AI tools in the performance of their duties for the firm. It covers generative AI (e.g., ChatGPT, Claude), analytics platforms, machine learning models, and automation tools.

AI tools may be used for the following business purposes:

- **Market Research & Competitive Intelligence:** Summarizing trends, industry benchmarks, and sector analysis.
- **Deal Sourcing:** Assisting in identifying potential acquisition or investment targets using data-driven tools.
- **Due Diligence Support:** Extracting, organizing, and analyzing data from large document sets, including contracts, financials, and compliance records.
- **Internal Process Automation:** Streamlining repetitive tasks such as scheduling, CRM updates, or data entry.
- **Content Creation:** Drafting non-confidential emails, marketing copy, or presentations with human oversight.
- **Client Briefings:** Producing first-draft summaries or dashboards for internal review before sharing with clients.

Prohibited Data Sharing with AI Tools

To protect client confidentiality, maintain regulatory compliance, and reduce security risks, the following types of information must never be shared with AI tools unless explicitly approved and protected by firm-approved systems:

Client Non-Public Information (NPI)

Includes deal terms, acquisition targets, valuation models, or undisclosed strategic plans.

Personally Identifiable Information (PII)

Names, emails, phone numbers, social security numbers, or any financial account information.

Confidential Financial Data

Internal financials, forecasts, earnings reports, cap tables, or due diligence materials.

Legal Documents

NDAs, contracts, term sheets, engagement letters, or regulatory filings.

Passwords or Security Credentials

Including logins, private keys, or access codes for any internal or client-facing systems.

Intellectual Property

Proprietary models, algorithms, market strategies, or training materials.

Anything Covered by a Confidentiality Agreement (NDA): When in doubt, assume it's confidential unless cleared by Legal or Compliance.

Even using AI tools for summarizing or drafting with this kind of data is prohibited unless the tool is secured, vetted, and explicitly approved for such use.

Use of Approved AI Services Only

To maintain control over data security and ensure compliance with firm policies, employees may only use AI platforms and services that have been explicitly approved by the company.

Guidelines:

- Only use AI tools tied to company-managed accounts (e.g., enterprise licenses, business-tier subscriptions).
- Do not use personal accounts or free/public versions of AI tools for any work-related tasks.
- All AI services must be reviewed by IT and/or Compliance before being approved for firm-wide or individual use.
- Access credentials for approved tools must be managed according to the company's password and access control policies.

Examples of non-approved usage:

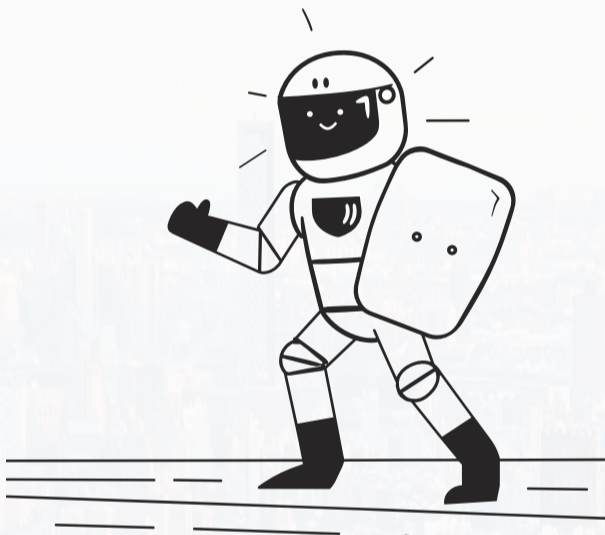
- Using personal ChatGPT, Gemini, or Claude accounts to process client information.
- Testing financial models or running due diligence queries on public-facing AI tools.
- Signing up for new AI apps or plugins without prior approval.

Unauthorized use of unvetted AI tools may result in disciplinary action and will be treated as a violation of the firm's data governance and cybersecurity protocols.

Data Privacy, Security, and Human Oversight

Data Privacy & Security

- No client PII, trade secrets, or financial documents may be entered into unsecured or non-enterprise AI platforms.
- Approved AI tools must meet our cybersecurity and compliance standards, including encryption and access controls.
- Always use firm-issued devices and secure networks when interacting with AI tools.



Human Oversight Requirement

AI-generated content must always be reviewed, verified, and edited by a qualified human before being shared with clients, published externally, or used in decision-making.

Compliance & Legal Considerations

Employees must comply with all applicable laws, including:

- SEC and FINRA guidance on AI use in financial services
- Data protection laws such as GDPR, CCPA, and HIPAA (if applicable)
- Non-disclosure agreements and confidentiality obligations

Training and Tool Approval Process

Training & Awareness

All staff must complete annual training on:



- Responsible AI usage
- Recognizing AI limitations and biases
- Data handling and client confidentiality with AI tools

Tool Approval Process

Before using a new AI platform or integration:



1. Submit a request to Compliance or IT.
2. Undergo risk assessment and legal review.
3. Receive written approval before use.

Monitoring & Audits



Usage of AI tools may be monitored for compliance, quality assurance, and continuous improvement. The firm reserves the right to audit tool usage and content.

Incident Reporting and Policy Violations

Incident Reporting

Any suspected misuse of AI or data leakage involving AI tools must be reported immediately to [Compliance Officer or IT Security Contact].



Policy Violations

Violations of this policy may result in disciplinary action, including revocation of AI access, formal warnings, or termination, depending on the severity.

Contact: For questions about this policy or tool approval, contact: [Name, Title, Email]

Acknowledgment of Receipt

I acknowledge that I have received, read, and understood the "AI Policy for M&A Advisory Firms."
I understand that it is my responsibility to comply with the policy and to seek clarification from management or compliance if I have any questions.

Employee Name: _____

Signature: _____

Date: _____