



AI Usage Policy

1. Purpose

This policy establishes guidelines for the ethical, secure, and lawful use of Artificial Intelligence (AI) tools within [Company Name]. It aims to promote innovation while safeguarding data privacy, intellectual property, and ensuring compliance with applicable laws and regulations.

2. Scope

This policy applies to all employees, contractors, and third-party collaborators who utilize AI tools in the course of their work with [Company Name]. It encompasses all AI technologies, including but not limited to:

- Generative AI (e.g., ChatGPT, DALL·E, MidJourney)
- Predictive analytics tools
- Machine learning algorithms
- Natural language processing applications
- AI-driven automation tools

3. Acceptable Use

- Authorized Tools: Only AI tools that have been reviewed and approved by the IT and Legal departments may be used. A list of authorized tools is maintained by the IT department.
- Use Cases: AI tools may be used to enhance productivity, automate repetitive tasks, and support decision-making processes, provided such use aligns with this policy.
- Prohibited Uses:
 - Legal document generation without review
 - Insertion of PII or trade secrets into third-party platforms
 - AI use that circumvents compliance or due diligence
 - Unauthorized surveillance or profiling
 - Use in regulated jurisdictions without legal counsel
 - Misleading use in customer-facing AI (e.g., undisclosed chatbots)
 - Generating content that is misleading, discriminatory, or violates company policies.
 - Using AI to make autonomous decisions without human oversight in critical areas such as hiring, legal judgments, or financial approvals

4. Data Privacy and Security

- Confidential Information: Do not input confidential, proprietary, or personally identifiable information (PII) into AI tools, especially those hosted by third parties, unless explicitly authorized.
- Data Handling: All data used with AI tools must comply with [Company Name]'s Data Protection Policy and relevant data protection laws, such as GDPR or CCPA.
- Third-Party Vendors: Ensure that third-party AI service providers have adequate security measures and data protection practices in place.



5. Intellectual Property

- Ownership: Outputs generated by AI tools are considered the property of [Company Name] if created in the course of employment.
- Third-Party Content: Avoid using AI tools to generate content that may infringe on third-party intellectual property rights. When in doubt, consult the Legal department.

6. Bias and Fairness

- Awareness: Recognize that AI tools may have inherent biases. Users must be vigilant and critical of AI outputs, especially in areas impacting individuals or groups.
- Mitigation: Regularly review and test AI tools for biased outcomes. Report any concerns to the Ethics Committee.

7. Accuracy and Accountability

- Human Oversight: AI-generated outputs must be reviewed by a human before implementation or dissemination.
- Responsibility: Users are accountable for the content and decisions made using AI tools. Reliance on AI does not absolve responsibility.

8. Compliance and Legal Considerations

- Regulatory Compliance: All AI tool usage must comply with applicable laws and regulations, including but not limited to data protection laws, intellectual property laws, and industry-specific regulations.
- Audit and Monitoring: [Company Name] reserves the right to monitor AI tool usage to ensure compliance with this policy.

9. Training and Awareness

- Education: Employees will receive training on the ethical and compliant use of AI tools.
- Resources: The IT and Legal departments will provide resources and guidance on approved AI tools and best practices.

10. Reporting and Enforcement

- Reporting Violations: Suspected violations of this policy should be reported to the Compliance Officer or through the anonymous reporting system.
- Consequences: Violations may result in disciplinary action, up to and including termination of employment or contracts.

Note

This policy is subject to periodic review and updates to adapt to evolving AI technologies and regulatory landscapes.

Expanded Prohibited Uses:

- Inputting client or customer data, trade secrets, or sensitive financial information into external AI platforms without prior legal review.
- Using AI to generate legal documents, contracts, or offer letters without review and approval by the Legal department.



- Employing AI in ways that violate nondisclosure agreements, contractual obligations, or regulatory compliance requirements.
- Utilizing AI to manipulate or fabricate evidence, records, or communications.
- Using AI tools to monitor, track, or profile employees or clients without explicit consent and a clear legal basis.
- Bypassing due diligence or standard compliance protocols by substituting AI for professional judgment or expert review.
- Deploying AI in customer interactions (chatbots, automated responses) that fail to disclose the use of artificial intelligence.
- Permitting AI to autonomously make hiring, firing, promotion, or disciplinary decisions.
- Relying on AI-generated research or outputs in regulatory filings, legal proceedings, or external audits without appropriate human verification.
- Using AI in jurisdictions or contexts where such use is prohibited or heavily regulated without appropriate legal counsel.