

AI Usage Policy

Effective Date

Version

Policy Owner

Approved by

1. Purpose

This **AI Usage Policy** establishes the rules for using artificial intelligence tools in connection with ("**Company**") business. Its purpose is to support responsible, secure, accurate, and transparent use of AI while protecting Company information, customers, employees, and other stakeholders.

This policy is an internal governance document. It does not create an employment contract or guarantee continued employment.

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and other individuals who use AI tools for or on behalf of the Company ("**Users**").

It applies to AI tools that generate, analyze, classify, summarize, translate, recommend, automate, or otherwise process content or data. This includes public AI services, Company-approved AI tools, AI-enabled software features, automated agents, and internally developed AI systems.

3. Definitions

For purposes of this policy:

"**AI Tool**" means a software product or feature that uses artificial intelligence, machine learning, generative AI, or similar technology to process information or produce outputs.

"**Company Data**" means information created, received, maintained, or controlled by the Company, including confidential business information, customer information, employee information, financial information, source code, product plans, and intellectual property.

“Confidential Information” means non-public information that the Company is required or expected to protect, whether it belongs to the Company or another party.

“Output” means content, analysis, recommendations, code, images, decisions, or other material produced by an AI Tool.

4. Permitted Use

Users may use Company-approved AI Tools for legitimate business purposes, including drafting, brainstorming, research support, summarization, translation, data analysis, workflow assistance, and administrative tasks.

Use of an AI Tool must be appropriate for the task, consistent with this policy, and subject to any additional requirements issued by the relevant department, Information Security, Legal, Human Resources, or the Company’s designated AI governance authority.

Users must use professional judgment and remain responsible for their work. AI Tools may assist with work, but they do not replace human review, accountability, or decision-making.

5. Approved Tools and Authorization

Users may use only AI Tools that have been approved by the Company for the intended use.

Before using a new AI Tool for Company business, the User must obtain approval from where required by Company procedures. Approval may depend on the tool’s security controls, data practices, contractual terms, access permissions, and intended use.

The Company may restrict, suspend, or withdraw approval for any AI Tool at any time.

6. Protection of Company Data

Users must protect Company Data and Confidential Information when using AI Tools.

Unless expressly authorized in writing by , Users must not enter, upload, connect, or disclose any of the following to an AI Tool:

- Personal data or sensitive personal data;
- Customer, supplier, employee, applicant, or business partner information;
- Confidential Information;
- Trade secrets, source code, credentials, passwords, security keys, or access tokens;
- Non-public financial, legal, operational, product, or strategic information;
- Information subject to contractual confidentiality obligations; or
- Information protected by law, regulation, or professional duty.

Users must follow the Company's data classification, information security, privacy, records retention, and confidentiality policies at all times.

7. Accuracy and Human Review

AI Outputs may be incomplete, inaccurate, outdated, biased, misleading, or unsuitable for the intended purpose. Users must review and validate Outputs before relying on, sharing, publishing, or using them.

Users must not present AI-generated content as verified fact without appropriate review. Where accuracy is important, Users must confirm information through reliable sources or qualified personnel.

A User remains responsible for all work submitted, communicated, approved, or acted upon using AI assistance.

8. Prohibited Uses

Users must not use AI Tools to:

- Make final decisions about hiring, promotion, compensation, discipline, termination, admission, credit, insurance, housing, healthcare, legal rights, or other high-impact matters without required human review and authorization;
- Generate discriminatory, harassing, threatening, defamatory, unlawful, or otherwise harmful content;
- Circumvent Company security controls, approval processes, or access restrictions;

- Create deceptive content, impersonate another person, or misrepresent AI-generated material as human-created where disclosure is required;
- Infringe another party's intellectual property rights or misuse copyrighted, proprietary, or confidential material;
- Conduct unlawful surveillance, profiling, or monitoring;
- Generate or distribute malicious code, phishing materials, security exploits, or instructions intended to compromise systems or data;
- Use AI Tools for personal commercial activities that conflict with the User's duties to the Company;
- or
- Use AI Tools in any manner prohibited by applicable law, Company policy, or contractual obligation.

9. Intellectual Property and Ownership

Users must not assume that AI Outputs are original, available for unrestricted use, or eligible for intellectual property protection.

Before using an AI Output externally or in a commercial product, service, marketing material, customer deliverable, or publication, the User must confirm that the intended use is permitted and obtain any required review from _____.

To the extent permitted by law and applicable agreements, work created by Users for Company business, including permitted AI-assisted work, belongs to the Company.

10. External Communications and Disclosure

Users must obtain required approval before using AI-generated content in external communications, public materials, customer-facing content, legal documents, financial communications, or statements made on behalf of the Company.

Users must disclose the use of AI when required by law, contract, Company policy, or the nature of the communication. Users must not use AI-generated audio, video, images, or text to mislead others about the source, authenticity, or approval status of a communication.

11. High-Risk and Sensitive Uses

Any proposed AI use involving personal data, sensitive information, automated decision-making, customer-facing services, security functions, regulated activities, or material operational impact requires review and written approval from , , and any other applicable internal function before deployment.

The Company may require testing, documentation, impact assessment, human oversight measures, monitoring, and periodic review before approving a high-risk AI use.

12. Incident Reporting

Users must promptly report suspected or actual AI-related incidents to . Reportable incidents include unauthorized disclosure of data, inaccurate or harmful Outputs, misuse of an AI Tool, suspected bias, security concerns, intellectual property concerns, or use that may violate this policy.

Users must preserve relevant information and cooperate with any investigation. The Company may suspend use of an AI Tool while it reviews an incident.

13. Training and Responsibilities

The Company may require Users to complete AI, data privacy, security, or responsible-use training before using certain AI Tools.

Managers are responsible for supporting compliance within their teams and escalating potential concerns. is responsible for maintaining approved-use guidance, coordinating reviews, and updating this policy as needed.

14. Monitoring and Audit

The Company may monitor, log, review, or audit AI Tool use to the extent permitted by applicable law and Company policy. Monitoring may include reviewing access, usage patterns, prompts, data connections, Outputs, and compliance with approval requirements.

15. Violations

Failure to comply with this policy may result in suspension of AI Tool access, corrective action, disciplinary action up to and including termination of employment or engagement, and other action permitted by applicable law or contract.

16. Policy Review and Amendments

The Company may amend, replace, or withdraw this policy at any time. The current version will be made available through .

Users are responsible for reviewing and complying with the current version of this policy.

Acknowledgment

I acknowledge that I have received, read, and understand this AI Usage Policy. I agree to comply with its requirements and to seek guidance when I am unsure whether a proposed use of an AI Tool is permitted.

Signatures

User

Name

Date

Signature

Company

Name

Date

Signature



This document is a PDF copy of **AI Usage Policy** template. You can edit it with **Jotform Sign** and convert to an eSign document with **Jotform Sign**.

 **Edit PDF**

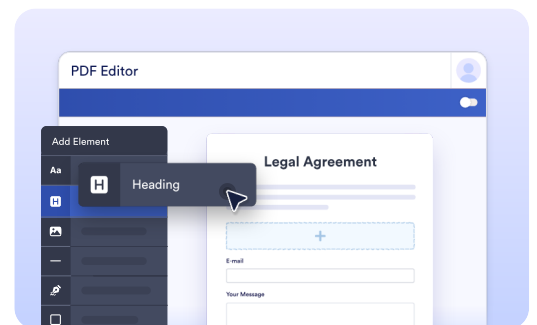
Learn More About Jotform PDF Products

Jotform offers powerful PDF solutions. Check them out below.

Jotform PDF Editor

Turn form submissions into PDFs automatically ready to download or save for your records.

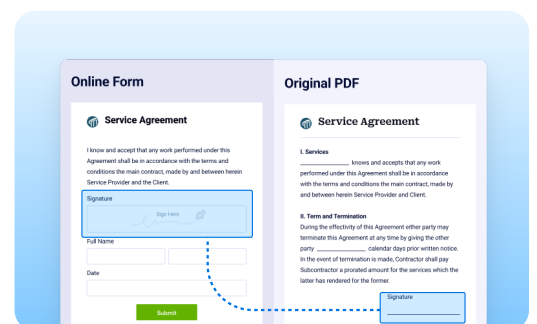
jotform.com/products/pdf-editor/



Smart PDF Forms

Convert your PDF files into online forms that are easy to fill out on any device.

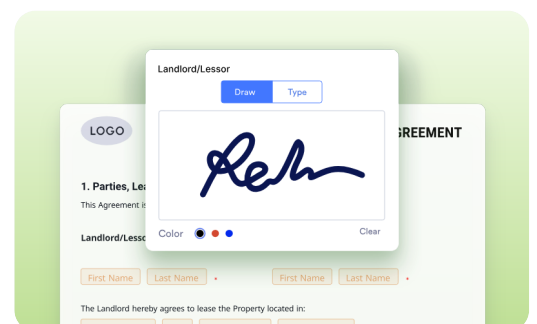
jotform.com/products/smart-pdf-forms/



Jotform Sign

Collect e-signatures with Jotform Sign to automate your signing process.

jotform.com/products/sign/



These templates are suggested forms only. If you're using a form as a contract, or to gather personal (or personal health) info, or for some other purpose with legal implications, we recommend that you do your homework to ensure you are complying with applicable laws and that you consult an attorney before relying on any particular form.