

General AI Usage Policy

[COMPANY NAME]

Purpose

[Company Name] uses artificial intelligence to support productivity, innovation, and business operations. This Policy establishes baseline expectations for everyday AI use. It is not a substitute for a formal AI governance program, and higher-risk or regulated AI use cases may require additional review, controls, or approval beyond what is described here.

Scope

This Policy applies to all employees, contractors, temporary staff, interns, and other personnel using AI on behalf of [Company Name].

It applies to:

- AI tools used for internal business purposes
- AI features embedded in approved software
- AI tools used to create, review, summarize, analyze, or transform business content
- AI-enabled workflows that may affect customers, employees, applicants, vendors, or other third parties

Roles & Responsibilities

[Company Name] assigns responsibility for oversight of this Policy to [Legal, Privacy, Security, IT, or other designated AI governance owner]. This role or function is responsible for maintaining this Policy, coordinating review of higher-risk AI use cases, and updating guidance as business practices, tools, and legal requirements evolve.

Managers are responsible for helping ensure that personnel understand and follow this Policy, and for escalating proposed uses of AI that may require additional review or approval.

All personnel are responsible for using only approved AI tools and features for company work, protecting Restricted Data, critically reviewing AI-generated output before use, obtaining required approvals, and promptly reporting suspected issues or misuse.

Definitions

AI For purposes of this Policy, “AI” means software or automated systems that generate, classify, recommend, summarize, analyze, or otherwise produce outputs based on user inputs, data, rules, or models. This



includes generative AI tools that can create text, code, images, audio, video, or similar outputs.

Restricted Data For purposes of this Policy, 'Restricted Data' means confidential, customer confidential, personal, sensitive, regulated, or otherwise legally or contractually restricted information.

Policy

Core Rules for AI Use

Employees may use AI tools for legitimate business purposes only, and only in ways that comply with this Policy and all other applicable company policies. At a minimum, employees must follow these rules:

- Use only approved AI tools or approved AI features within company-approved software
- Do not enter Restricted Data into public or unapproved AI tools.
- Do not use personal AI accounts for company work unless expressly authorized
- Treat AI output as a draft or aid, not as a final answer
- Review AI-generated output for accuracy, completeness, bias, appropriateness, and fit for purpose before relying on it, sharing it, or publishing it
- Do not use AI to make up facts, citations, approvals, test results, legal conclusions, or other information that appears authoritative but has not been verified
- Do not use AI in ways that are deceptive, discriminatory, unlawful, unsafe, or inconsistent with company values
- Follow any disclosure, attribution, or approval requirements that apply when AI-generated content is shared externally

Uses That Require Additional Approval

The following uses require review and approval from the appropriate internal team before deployment or use:

- Using a new AI tool or vendor that has not gone through company review
- Uploading company confidential, customer, personal, sensitive, regulated, or proprietary information into an AI tool
- Training, fine-tuning, or customizing an AI model using company data, customer data, or personal data
- Using AI for customer-facing outputs, product features, or automated workflows
- Using AI to support decisions involving hiring, employment, promotions, discipline, compensation, credit, eligibility, legal rights, safety, or similarly high-impact matters
- Using AI to generate or approve legal, privacy, security, financial, or compliance conclusions without qualified human review



- Using AI in ways that could affect contractual commitments, public claims, product representations, or regulated communications

These uses represent higher-risk AI activity. If [Company Name]'s AI use increasingly falls into these categories, leadership should evaluate whether a more formal AI governance program or framework is needed in addition to this Policy. Requests for approval should be routed through [Legal, Procurement, IT, Security, Etc.].

Data Handling and Confidentiality

All use of AI must comply with [Company Name]'s confidentiality, privacy, security, records, and data classification requirements.

Employees must:

- Use the minimum data necessary for the task
- Do not enter Restricted Data into AI tools unless the tool and use case have been specifically approved by [Legal, Procurement, IT, Etc.]
- Confirm with [GRC, Procurement, Legal, Privacy, IT] that any approved enterprise AI environment has appropriate privacy, security, and contractual protections
- Handle outputs containing company, customer, or personal information in accordance with existing company policies
- Stop use and seek guidance if there is any uncertainty about whether data can be used in an AI tool

Intellectual Property and Content Use

Employees must use AI in a way that respects intellectual property, contract, and licensing obligations.

Employees must not:

- Upload materials to AI tools if doing so would violate confidentiality, contract terms, export restrictions, or third-party rights
- Assume AI-generated content is free of copyright, trademark, trade secret, or other legal risk
- Use AI-generated content externally without appropriate review when the content may be customer-facing, branded, technical, legal, or commercially significant

Where needed, employees must obtain review from Legal, Marketing, Product, or other appropriate stakeholders before use.



Human Review and Accountability

Humans remain responsible for business decisions, customer communications, compliance judgments, and final work product.

Using AI does not transfer accountability away from the employee, team, or business owner. Anyone using AI is responsible for:

- Understanding the task well enough to review the output critically
- Verifying key facts, conclusions, and recommendations
- Escalating concerns, errors, or unexpected behavior
- Ensuring that required approvals are obtained before use

AI may assist work. It does not replace human judgment.

Vendor and Tool Review

Before a new AI tool is adopted for business use, [Company Name] should evaluate the tool's:

- Security and access controls
- Privacy and data handling practices
- Confidentiality protections
- Model training and retention terms, where relevant
- Ability to support legal, contractual, and compliance requirements

This review is intended to catch common risks for everyday AI tool use. Vendors supporting higher-risk, regulated, or customer-facing AI use cases should go through a more rigorous third-party risk assessment process. No employee may independently commit the company to a new AI vendor or service without following the normal procurement and review process.

Monitoring, Reporting, and Incidents

Employees must promptly report any suspected AI-related issue, including:

- Data exposure or inappropriate sharing
- Biased or harmful outputs
- Misleading or fabricated outputs
- Security concerns
- Improper use of an AI tool
- Unexpected tool behavior that could create legal, operational, or customer risk



Reports should be made through [insert incident channel, manager, privacy team, security team, legal team, or other reporting path].

Training

[Company Name] may require training on approved AI use, data handling, human review expectations, and role-specific restrictions, including as part of onboarding and on an [timeframe] basis thereafter. Employees are expected to complete required training and follow related guidance. Managers should ensure new tools, workflows, or role changes involving AI are reflected in relevant training.

Violations

Violations of this policy may result in removal of tool access, corrective action, disciplinary action, or other appropriate response, consistent with company policy and applicable law.

Review and Updates

AI technology, business practices, and legal expectations are changing quickly. [Company Name] may review and update this Policy periodically to reflect changes in technology, risk, law, and business operations.



Revision History

Version	Date	Editor	Approver	Description of Changes	Format