



Sample: Artificial Intelligence (AI) Acceptable Use Policy

1. Purpose and Scope

This Artificial Intelligence (AI) Acceptable Use Policy establishes expectations and requirements for the responsible, ethical, and secure use of AI technologies by employees and contractors. The goal of this policy is to enable productivity and innovation while protecting the organization, its members, partners, and staff from legal, ethical, operational, and reputational risk.

This policy applies to all AI-enabled tools, whether standalone (e.g., generative AI systems) or embedded within business software (e.g., productivity platforms, conferencing tools, marketing platforms).

2. Guiding Principles

AI may be used to support human work, not replace human judgment. All AI-assisted work remains the responsibility of the individual using the tool.

Use of AI must:

- Comply with applicable laws, regulations, and professional standards
- Protect confidential, proprietary, and regulated information
- Avoid misleading, discriminatory, or biased outcomes
- Include appropriate human review and accountability

3. Risk-Tiered AI Use Framework

AI use cases are categorized into four risk tiers. Approval and oversight requirements depend on the tier.

Tier 1 – Low Risk (Permitted Without Prior Approval)

These uses support productivity and do not involve sensitive data or external reliance.

Examples:

- Grammar, spelling, and tone improvement
- Summarizing non-confidential documents or meetings



- Brainstorming ideas or outlines
- Drafting internal notes or learning materials

Conditions:

- No confidential, proprietary, or personal data may be entered
- Output must be reviewed by the user
- AI-generated content may not be used verbatim as final external work product

Tier 2 – Moderate Risk (Manager Approval Required)

These uses influence deliverables or external communications.

Examples:

- Drafting marketing or educational content
- Preparing presentations, blogs, or social media drafts
- Analyzing non-sensitive datasets

Conditions:

- Manager approval for the use case
- Clear human authorship and editing
- Fact-checking and bias review required
- Disclosure of AI assistance where appropriate

Tier 3 – High Risk (IT and Legal Approval Required)

These uses carry heightened legal, regulatory, or reputational risk.

Examples:

- Member-facing guidance or educational materials relied upon for decision-making
- Automated data analysis influencing policy, pricing, or strategy
- Integration of AI tools with internal systems

Conditions:

- Written approval from IT and Legal



- Documented human oversight
- Defined data handling safeguards
- Formal review before release

Tier 4 – Prohibited Uses

The following uses are strictly prohibited:

- Inputting confidential, proprietary, or regulated data
- Making employment-related decisions
- Representing AI-generated output as fully human-authored work
- Creating content intended to bypass intellectual property protections
- Deploying AI systems autonomously without human oversight

4. Data Protection and Confidentiality

Users must never input:

- Personally identifiable information (PII)
- Confidential or proprietary organizational data
- Credentials or security information
- Information protected by data privacy laws

All AI use must comply with applicable data protection requirements.

5. Intellectual Property and Attribution

AI may be used as an assistive tool. Human contribution must remain substantial. Final ownership and authorship determinations will follow applicable law and organizational guidance.

AI-generated output must be reviewed, edited, and validated by a human before use.

6. Transparency and Disclosure

Where AI materially contributes to external-facing content, its use must be disclosed in accordance with organizational standards.



7. Training and Accountability

Employees must complete required AI acceptable use training. Misuse of AI may result in disciplinary action.

8. Governance and Review

This policy will be reviewed annually. Oversight responsibility rests with designated leadership, in coordination with IT and Legal.