

AI Acceptable Use Policy

Purpose

Generative AI and other AI systems can improve the quality and speed of work, but they can also expose confidential information, produce wrong or biased output, and create legal and intellectual property risk. This policy sets the rules that let Your Organization gain the benefits while keeping control of its data and its decisions.

Scope

This policy applies to all workforce members of Your Organization who use AI systems for company work, including chat assistants, code assistants, image and audio generators, meeting transcription and summarization tools, AI features embedded in other software, and AI services accessed through an API. It covers tools Your Organization provides and tools a person brings, whether free or paid. It does not govern the design and release of AI features in Your Organization's own products, which falls under the AI governance program and the Secure Development Lifecycle Policy.

Roles and responsibilities

- **The AI governance owner (or security team)** maintains the list of approved AI tools, reviews requests, and owns this policy.
- **Managers** make sure their teams use only approved tools for the approved purposes.
- **Users** are personally accountable for what they submit to an AI system and for the output they use.
- **Legal and privacy** advise on intellectual property, contractual, and privacy implications.

Requirements

1. Approved tools

- Use only AI tools on the approved list for company work. The list records for each tool the permitted data classifications, the permitted use cases, whether inputs are retained or used to train models, and the contract and security review outcome.
- New tools and new AI features in existing tools are requested through the process owned by the AI governance owner and are reviewed under the Vendor Risk Management Policy.
- Sign in to approved tools with company accounts and single sign-on. Do not use personal accounts for company work.

2. Data that may be entered

- Public information may be entered into any approved tool.
- Internal information may be entered only into tools approved for internal data.

- Confidential data, customer data, personal information, credentials, secrets, source code, and regulated data (for example, CUI, health, or payment data) may be entered only into tools expressly approved for that class of data, under terms that prevent the vendor from retaining the data or training on it.
- Never enter passwords, API keys, private keys, or authentication tokens into an AI system.

3. Human accountability and review

- AI output is a draft. The person who uses it is responsible for checking it for accuracy, bias, security, and fit before relying on it or sharing it.
- AI output must not be the sole basis for a decision that significantly affects a person, such as hiring, firing, discipline, credit, or access to services. A qualified human makes and records those decisions.
- AI-generated code follows the same review, testing, and scanning rules as other code. Reviewers must understand it before approving it.
- Where output is shared outside Your Organization and AI materially shaped it, apply any disclosure rule the business or the law requires.

4. Intellectual property and confidentiality

- Do not submit material that Your Organization does not have the right to use, or material that belongs to a customer or partner, unless the contract allows it.
- Check that output does not reproduce third-party copyrighted or licensed material, and follow the license terms of any generated code or assets.
- Consult legal before using AI output in a product, a contract, a regulatory filing, or public statements.

5. Prohibited uses

Users must not:

- Use AI to generate or spread deceptive, harassing, discriminatory, or unlawful content.
- Use AI to impersonate a person, or to produce deepfakes of real people without their consent.
- Use AI to bypass security controls, develop malware, or probe systems without authorization.
- Use unapproved agentic tools that take actions in company systems, such as sending email or changing records, or give an AI agent standing credentials.
- Use AI note-takers or recording features in meetings without the consent required by law and by the meeting participants.

6. Incidents and concerns

Report suspected data exposure through an AI tool, harmful or unsafe output, or a misuse of AI to the security team immediately. Incidents are handled under the Incident Response Plan. Staff can raise concerns about AI use without retaliation.

7. Monitoring

Your Organization may monitor use of AI tools on company systems and accounts, within the limits of applicable law, to enforce this policy and detect data leakage.

8. Training

Workforce members complete AI-use training on hire and annually. The training covers data handling, verification of output, and recognized limitations of AI systems.

Exceptions

Exceptions require written approval from the AI governance owner and the security team, state the tool, data, and purpose, and expire after at most twelve months.

Enforcement

Violations may result in loss of access to AI tools and disciplinary action in line with the Acceptable Use Policy.

Evidence

Evidence of operation includes the approved tool list, request and review records, vendor terms, training records, and incident records.

Review cadence

Because AI tools and the rules around them change quickly, this policy is reviewed at least every six months by the AI governance owner, security team, privacy, and legal.

Effective date: [the date this policy takes effect]