

[Company Name] AI Acceptable Use Policy

Free template from CIO Support, published by LAN Service Group, Inc. Version 1.0, October 2026.

How to use this template (delete this box before publishing)

- Replace every [bracketed field] with your own details. Before you publish, delete this box, the grey guidance notes, the "Free template from CIO Support" line under the title and the template footer.
- Keep it short. Employees should be able to read it in a few minutes. Put ownership, vendor review and risk management in your separate AI governance policy, and make sure the two do not contradict each other.
- Have your own legal and HR advisers review it before adoption. This template is general guidance, not legal advice, and does not address the specific laws, contracts or regulators that apply to your organization.
- You may copy, edit and use this template inside your organization. Explanation of each section: <https://cio.support/ai/ai-acceptable-use-policy-template/>

Field	Value
Policy owner	[Name, title]
Approved by	[Senior leader accountable for AI governance]
Effective date	[Date]
Next review date	[Date, no more than 12 months after the effective date]
Version	[1.0]

1. Purpose

[Company Name] encourages the productive use of artificial intelligence (AI) tools. This policy sets the rules that let you use AI at work without exposing company, customer or employee information, and without passing on AI output that has not been checked.

2. Scope

This policy applies to all employees, contractors, temporary staff and interns ("you") who use AI tools for [Company Name] work, on company devices or on personal devices. "AI tool" includes:

- Chat assistants and AI search tools.
- AI features built into software the company already licenses, such as email, documents, CRM or meeting tools.
- Coding assistants.
- Browser extensions and plug-ins that read, summarize or rewrite content.
- Meeting note-takers, transcription and recording bots.
- Image, audio and video generators.

3. Approved AI tools and accounts

Use only the AI tools listed below, and only through company-managed accounts that you sign in to with your company credentials [through single sign-on]. Do not use personal AI accounts, free or paid, for company work.

Guidance: list each approved tool, what it may be used for and the highest data classification allowed in it. Keep the live list where staff can find it and update it without reissuing the policy.

Approved tool	Approved uses	Highest data allowed	Account
[Tool name]	[e.g. drafting, summarizing internal documents]	[e.g. Internal]	Company-managed
[Tool name]	[e.g. code suggestions in approved repositories]	[e.g. Confidential]	Company-managed
[Tool name]	[]	[]	Company-managed

The current approved list is kept at [location or link] and is maintained by [owner].

Do not connect an AI app, plug-in or extension to company email, files, calendars or other systems, and do not grant it access when asked to sign in or approve permissions, unless it is on the approved list for that use.

4. Data rules

Before you enter anything into an AI tool, check its classification under [Company Name]'s [data classification policy] and the limit set for that tool in section 3.

Guidance: use your own classification levels. The four below are an example only.

Classification	Examples	May go into
Public	Published marketing, public website text	Any approved tool
Internal	Internal procedures, non-sensitive meeting notes	Approved tools rated Internal or higher
Confidential	Financials, contracts, customer lists, source code	Only tools approved for Confidential data
Restricted	Regulated or legally protected data (see list below)	Never for the first list below; the second list only with written approval as described below

Never type, paste or upload the following into any AI tool. There are no exceptions:

- Passwords, API keys, access tokens, private keys or other credentials.
- Payment card numbers, bank account numbers, Social Security numbers or other government ID numbers.

Do not type, paste or upload the following into any AI tool unless [owner] has approved a specific tool and environment for that data in writing, after [Legal / Compliance] confirms that the required contracts and safeguards are in place. Without that written approval, the answer is no:

Guidance: examples of what to confirm include a HIPAA business associate agreement with the vendor before any protected health information is used, an environment that meets your DFARS 252.204-7012 and NIST SP 800-171 obligations before any CUI is used, and an export-control review before any ITAR or EAR technical data is used. Have counsel confirm what applies to you.

- Health information about identifiable people, including protected health information (PHI).
- Controlled unclassified information (CUI) and export-controlled technical data (ITAR or EAR).
- Personal information about customers, employees or job applicants beyond what the approved use requires.

- Unpublished inventions, trade secrets and [other sensitive intellectual property].
- Information a customer, partner or other third party gave us under a confidentiality obligation, or that a contract says may not be shared with outside service providers.

If you are not sure how information is classified, treat it as Restricted and ask [contact].

5. Human review and accountability

You are responsible for anything you produce with AI help, exactly as if you had written it yourself. AI tools can be confidently wrong, invent sources and produce insecure code.

- Check facts, figures, names, citations and links against a reliable source before you rely on them.
- A person must review AI output before it goes to a customer, is used in a contract, is sent to a regulator, is deployed as production code or becomes part of a regulated record.
- AI output must never be the sole basis for decisions about a person's hiring, pay, promotion, discipline or termination, or a customer's eligibility for [products or services]. A person must make, and be accountable for, the final decision. Any AI tool used to support these decisions needs prior [HR / Legal] approval.

Guidance: rules on automated decision-making in employment and consumer decisions differ by jurisdiction. Ask counsel which apply to you before approving any such tool.

6. Transparency

- Disclose AI assistance when [e.g. a customer, regulator or contract requires it, or when content is published under a person's name].
- Do not use AI to impersonate a real person, or to create content intended to mislead.
- Before using a meeting note-taker, transcription or recording tool, follow [Company Name]'s rules on notifying participants and obtaining consent, and applicable law.

Guidance: some states require consent from every participant before a call is recorded. Check the rules where your attendees are located.

7. Requesting a new AI tool

To request a tool, or a new use for an approved tool, contact [owner or request link]. Do not use the tool for company work until it is approved. The review will consider, at minimum:

- Whether the vendor uses our inputs or outputs to train its models, and whether that can be turned off.
- How long the vendor keeps data, where it is stored, and whether we can delete it.
- Whether the company can manage accounts centrally, require company sign-in and remove access.
- Which data classifications the tool may receive, and any contract terms required first.

Requests are normally answered within [number] business days.

8. Reporting problems

Report to [contact, email or phone] within [number] hours if:

- You entered information into an AI tool that this policy does not allow, including by accident.
- AI output that was used or sent turns out to be wrong in a way that could cause harm.
- An AI tool behaves unexpectedly, such as showing someone else's data or asking for credentials.

Prompt self-reporting helps us limit the damage. [Optional: An employee who promptly reports their own honest mistake will not be disciplined for that mistake alone.]

Guidance: include the optional sentence only if HR and Legal approve it, because employees may treat it as a binding commitment.

9. Monitoring and violations

[Company Name] may monitor the use of company accounts, devices and networks, including AI tools, as permitted by law and [Company Name]'s [monitoring or electronic communications policy]. Violations of this policy are handled under [disciplinary policy] and may lead to loss of access to AI tools or other disciplinary action.

10. Review

[Owner] reviews the approved-tool list at least [quarterly] and this policy at least once a year, and after any significant change in the tools we use, our legal or contract obligations, or a reported incident. You will be asked to acknowledge the policy again after material changes.

11. Related policies

[AI governance policy] · [Data classification policy] · [Information security policy] · [General acceptable use of IT policy] · [Confidentiality / intellectual property agreement]

Acknowledgment

I have read and understand the [Company Name] AI Acceptable Use Policy and agree to follow it. I understand that I am responsible for the AI output I use in my work.

Name	
Signature	
Job title	
Date	