Astraea
PARTNERS

TEMPLATE · ASTRAEA PARTNERS

AI Acceptable Use Policy Template

A ready-to-adapt baseline policy that sets out which AI tools can be used, with what data, with what oversight, and who is accountable.

Version of October 19, 2026

How to use this template

Replace the text in brackets, remove what doesn't apply, and align the data classification levels with the ones your organization already uses. Have legal, risk, and security review it before approval.

> This template is a general starting point. It is not legal advice and must be adapted to the laws and contracts that apply to your organization.

1. Purpose

This policy sets out how [Organization name] allows the use of artificial intelligence (AI) tools, including generative AI, so we can benefit from them while protecting

information, people, and the organization.

2. Scope

It applies to all staff, contractors, and third parties who use AI tools to work with [Organization name] information, on company or personal devices.

3. Principles

1. **People are accountable.** Whoever uses an AI tool is responsible for the result they deliver.
2. **Data comes first.** No data is shared with an AI tool unless its classification allows it.
3. **Transparency.** We disclose when content delivered to clients or third parties was substantially generated with AI.
4. **Proportionality.** The higher the impact of a use, the stronger the controls and oversight.

4. Approved tools

- Only tools on the approved tools list, published at [location], may be used.
- To propose a new tool, submit a request to [responsible role or committee], which assesses security, privacy, data-use terms, and the vendor.
- Personal or free AI accounts are not used for organizational information unless they are on the approved list.

5. Data use by classification

Classification	Can it be used with AI tools?
Public	Yes, with any approved tool.
Internal	Yes, only with tools approved for internal use.
Confidential	Only with tools expressly approved for this level, under a contract that prevents the data from being used to train models.
Restricted (sensitive personal data, credentials, trade secrets)	No, unless authorized in writing by [responsible role].

6. Permitted and prohibited uses

Permitted, with approved tools and in line with section 5: drafting and summarizing text, generating ideas, supporting information analysis, translating, writing and reviewing code, and preparing document drafts.

Prohibited:

- Making automated decisions that affect people (hiring, credit, sanctions, access to services) without human review.
- Entering credentials, passwords, or access keys.
- Creating misleading or discriminatory content, or impersonating a person.
- Using unverified AI output in legal, financial, or regulatory documents.
- Bypassing the organization's security controls.

7. Human oversight and quality

- All AI output is reviewed before use; the higher the impact, the more rigorous the review.

- Data, figures, quotes, and references generated with AI are checked against a reliable source.
- High-impact uses are recorded in the AI use inventory and have a designated owner.

8. Roles and responsibilities

- **[AI committee or owner]:** approves tools and high-impact uses, and maintains the inventory.
- **Information security:** assesses tools and monitors their use.
- **Managers:** make sure their teams know and follow this policy.
- **Every user:** uses AI in line with this policy and reports incidents.

9. Training

All staff receive training on this policy when they join and a refresher at least once a year.

10. Incidents

Any data exposure, harmful output, or misuse of an AI tool is reported immediately to [reporting channel], following the organization's incident management process.

11. Compliance and review

Breaches of this policy are handled under [internal rules or code of conduct]. The policy is reviewed at least once a year or after significant changes in technology or regulation.

Approved by: [approving body] · **Date:** [date] · **Version:** [number]

Next step

A policy is the first step. To make it work you need a use inventory, a risk assessment, and proportionate controls — which is what we build in the AI Risk Quick Scan and the 90-Day AI Adoption Program.

Astraea Partners · hola@astraea.example · https://astraea.example/en/tools/ai-acceptable-use-policy/
Version of October 19, 2026. This document is the property of Astraea Partners S.A. You may use and adapt it freely within your organization; if you share it, please credit Astraea as the source.