



Community Library

ISO 27001 AI Use Guardrails

Ten rules for using AI tools at work without leaking data or trusting a bad answer.

4

Rules

4

Use

2

Check

1.0 · 2026-10

itrygg.com

How to use this checklist

An AI tool can send company information somewhere you did not approve, or hand back an answer nobody checked. Give these rules to the people who approve the tools and the people who use them. Each rule also names the proof your ISO/IEC 27001 program should already be able to show.

- 1. Work the parts in order: set the rules, use the tool, then keep it in check.
- 2. The Proof line is the record your program keeps. If you cannot produce it, the rule is not in place.
- 3. If your classification labels differ from Confidential and Restricted, use your own labels.
- 4. References point to ISO/IEC 27001:2022 Annex A controls, for example A.5.10.
- 5. This is guidance. Adapt it to your contracts and the privacy rules that apply to you.

Rules	Use	Check
Before anyone uses a tool	While they use it	After the rules are set

Set the rules

The approved list, the accounts, the vendor check, and the briefing exist before access.

- ☐ Publish the list of AI tools and accounts staff may use, and name who approves a new one. A.5.10, A.5.23

Proof: The approved list, with the person who approves additions.

- ☐ Use company-managed accounts with single sign-on, and turn off training on your data where the tool offers that setting. A.5.16, A.5.23

Proof: Account record showing company management, single sign-on, and the training setting where it exists.

- ☐ Before you sign, check where the vendor stores the data, how long they keep it, and who can see it. A.5.19, A.5.20

Proof: Vendor check on file before the tool is approved.

- ☐ Brief everyone on these rules before they use an AI tool for work. A.6.3

Proof: Attendance or completion record dated before access.

Use it safely

The data matches the tool, secrets stay out, answers get checked, and a person still decides.

- ☐ Put Confidential or Restricted data only into a tool approved for that label. A.5.12, A.5.13
Use your own labels if they differ.

Proof: The approved list says which label each tool may receive.

- ☐ Keep passwords, API keys, and customer personal data out of prompts unless the tool is approved for that data. A.5.34, A.8.11

Proof: The rule in the briefing, and the approved list showing which tools may receive that data.

- ☐ Check facts, figures, and citations before you rely on them, and review AI-written code the same way you review any other code. A.8.28

Proof: Review note on the work that used an AI draft, including code.

- ☐ A named person approves decisions that affect people. AI can draft and suggest. A.5.31

Proof: The decision record names the person who approved it.

Keep it in check

Unapproved tools get found, and a paste into the wrong tool is reported.

- ☐ Find unapproved AI tools, extensions, and meeting bots, and offer an approved option.

A.5.9, A.8.16

Proof: Review record of what was found, and the approved option offered.

- ☐ Report data pasted into the wrong tool, or harmful output, as a security event.

A.6.8, A.5.24

Proof: Event record, or a note that none was reported in the period.

Want the approved list and the event to live in the program, not in a chat thread?

Trygg keeps the approved tools, the briefing, and the proof in one place.

[Book a demo](https://itrygg.com/#demo) (itrygg.com/#demo)

[ISO 27001 Preparation Checklist](https://itrygg.com/community/library/iso-27001-preparation-checklist) (itrygg.com/community/library/iso-27001-preparation-checklist)

Portal demos follow a mutual NDA.

isms@itrygg.com

This checklist is guidance, not a substitute for the ISO/IEC 27001:2022 standard. Purchase the standard from ISO or your national standards body. Certification decisions are made only by accredited certification bodies.

© 2026 Trygg, Inc.