

GUIDE · TECHNOLOGY STRATEGY

An AI acceptable use policy should tell staff what they may do with AI, who decides and when it is reviewed.

Published 18 October 2026 6 min read



Photo: Tanja Tepavac, Unsplash

IN BRIEF

An acceptable use policy tells staff which AI tools they may use, for what and with which data, and it names who decides.

Start from the risks, set clear data limits, name an owner and an approval route, and require records and training.

Set a review date, because the standards and laws behind the policy are still changing.

Before you start

An acceptable use policy is the short document that tells staff which AI tools they may use, for what purposes and with which information. In our view it is the first AI control to put in place, because staff may already be using AI tools at work.

This guide is for IT managers and the executives they report to. The sources below describe what such a policy should cover rather than offering a sample to copy, and this guide follows them.

The idea has a formal basis. NIST's Generative AI Profile, released in 2024, asks organizations to establish transparent acceptable use policies that address illegal use of generative AI. It also asks them to define such policies for chatbots and decision-making tasks, including criteria for the kinds of queries an application should refuse.

Start with the risks

A policy is easier to defend when each rule answers a named risk. The Government of Canada's guide says these tools can generate inaccurate content, amplify biases and violate intellectual property, privacy and other laws. It adds that institutions must evaluate the risks before they start using them.

NIST's profile is more detailed and lists 12 risks, among them data privacy, information security, intellectual property and harmful bias. It also defines confabulation as confidently stated but erroneous or false content, which is the reason staff should check what a tool produces.

Set limits on data and tools

The data rule is the one staff most need to hear. The Government of Canada's guide says public servants must not input personal information into publicly available online generative AI tools, while personal information may go into systems the government controls or configures, where the appropriate privacy and security controls are in place.

In our view, a private organization can draw the same line between tools it manages and tools it does not. The policy should say where that line sits.

Canada's privacy regulators add a legal frame. Their joint principles, issued on 7 December 2023, include necessity and proportionality, accountability, and limits on collection, use and disclosure.

Name an owner and an approval route

Every rule needs someone who answers for it. On approval, the Government of Canada's guide says to seek the approval of the institutional chief security officer before using, procuring or deploying generative AI for protected or sensitive information, and to consult privacy officials about whether a Privacy Impact Assessment is needed.

The UK Government's playbook advises an AI review board or a program-level board, and says humans should validate any high-risk decisions influenced by AI. NIST describes governance as a cross-cutting function that is infused throughout AI risk management.

Our view is that one named executive should own the policy, with the IT manager running it day to day and legal, privacy and security staff consulted on every new tool.

A checklist of what to cover

Use this list as the outline of the policy.

1. **Purpose and scope.** Say who the policy covers. NIST asks for acceptable use policies to be updated to address contractors, consultants and other third-party personnel, as well as proprietary and open-source tools.
2. **Approved tools, prohibited uses and the approval route.** List the tools staff may use, name the uses that are never allowed, starting with illegal ones, and say how to request a new tool.

3. **Data limits.** Say what information may never be entered into tools the organization does not manage, and name the categories.
4. **Checking output.** The Government of Canada's guide says to always review AI-generated content and not treat it as authoritative, and to indicate when content was produced by generative AI.
5. **Records and training.** The same guide says that if use of these tools is an activity of business value, you must document it. Say what training staff must complete and how often.
6. **Suppliers and partners.** NIST's framework expects policies and procedures that address AI risks associated with third-party entities, including infringement of a third party's intellectual property.
7. **Owner, exceptions, reporting and review.** Name the owner, say how to ask for an exception and where staff report a problem, and state when the policy will next be reviewed.

Train people and keep records

A policy that nobody has been taught is hard to enforce. The Government of Canada's guide says institutions should ensure that employees can access and take training on the effective and responsible use of generative AI tools. NIST's framework expects that personnel and partners receive AI risk management training suited to their duties.

In the European Union, AI literacy is a legal duty for providers and deployers. Under the AI Act, a deployer is any person or body using an AI system under its authority, except in personal non-professional activity. Article 4 of the original 2024 text says providers and deployers shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff.

The European Commission's guidance says that there is no need for a certificate and that an organization can keep an internal record of trainings. The Commission also says the duty has applied since 2 February 2025, and that national market surveillance authorities supervise and enforce it from August 2026.

The Commission's AI Act Service Desk now shows a consolidated text with different wording, which supports the development of AI literacy and does not require a guaranteed level for any individual. Check the current text before relying on either version.

Keep the policy current

Set a review date and a trigger for earlier review, such as a new tool, a new law or an incident. The sources behind the policy are moving.

NIST's framework was released in January 2023 and is voluntary, and NIST says it is being revised as part of the White House AI Action Plan. The OECD's principles were adopted in May 2019 and updated in May 2024.

A management system standard can help if you want the policy to sit inside a wider program. ISO/IEC 42001 specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving an AI management system within an organization. The standard itself is paid, so we describe only its published scope.

What this means for you

1. Find out which AI tools staff already use, and ask before you restrict anything.
2. Name one executive owner and an approval route.
3. Write the data limits first, since they carry the most risk.
4. Use the checklist above as the outline, and keep the policy to a few pages.
5. Schedule training, start the records and set the first review date.

Our technology strategy service helps leaders draft and govern AI policies that fit their organization. If you would like to start, request a briefing.

SOURCES

Government of Canada, Treasury Board of Canada Secretariat [Guide on the use of generative artificial intelligence](#) 2026

Office of the Privacy Commissioner of Canada and provincial and territorial counterparts [Principles for responsible, trustworthy and privacy-protective generative AI technologies](#) 2023

NIST [Artificial Intelligence Risk Management Framework \(AI RMF 1.0\)](#), NIST AI 100-1 2023

NIST [AI Risk Management Framework overview page](#) 2026

NIST [Generative Artificial Intelligence Profile, NIST AI 600-1](#) 2024

UK Government, Government Digital Service [Artificial Intelligence Playbook for the UK Government](#) 2025

European Union [Regulation \(EU\) 2024/1689 \(AI Act\)](#) 2024

European Commission [AI Literacy, Questions and Answers](#) 2026

European Commission, AI Act Service Desk [Article 4, AI literacy](#) 2026

OECD [OECD AI Principles](#) 2024

IEC [ISO/IEC 42001:2023, Information technology, Artificial intelligence, Management system](#) 2023

DISCUSS THIS WITH US

To discuss this with Consier Technologies, visit consiertech.com/contact/.