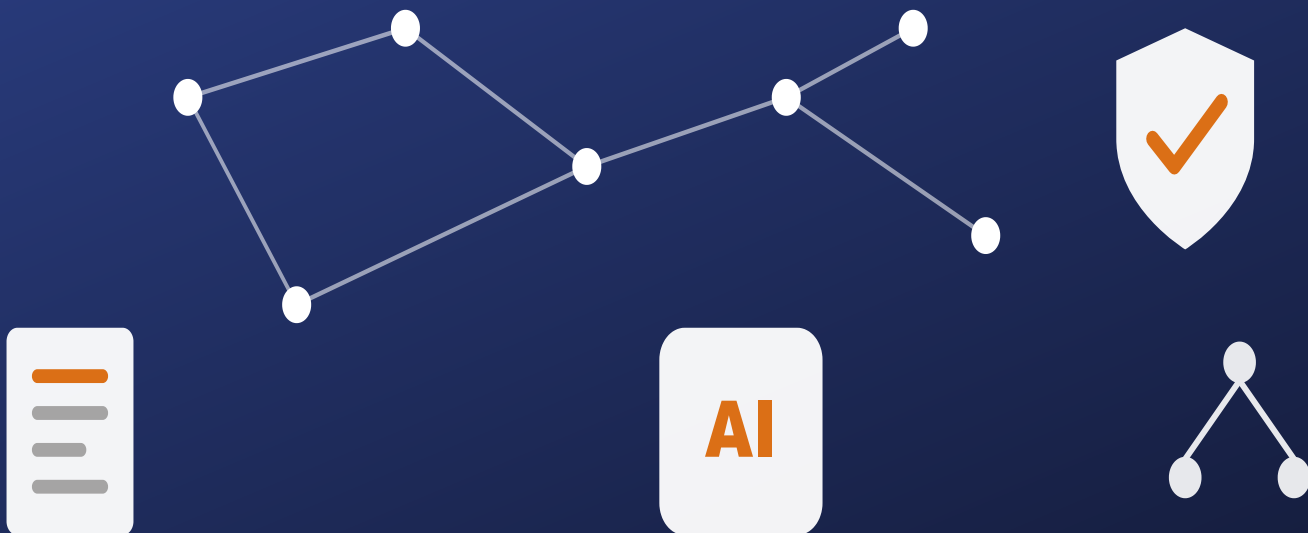


AI Best Practices for Business Leaders & Management

AI adoption is a **governance, security, and risk decision** — not just a productivity choice. These best practices help your organization scale AI safely.

Last Updated: 2026-07-29



1. Treat AI Adoption as a Governance Decision, Not Just a Tool Choice

Your staff are very likely already using ChatGPT, Claude, Copilot, or similar tools to draft emails, summarize documents, or analyze data — whether or not the business has formally approved it.

- Assume AI is already in use somewhere in your organization, sanctioned or not.
- Decide, in writing, which tools are approved for company work, and who owns that decision.
- Revisit the decision on a schedule — this space changes every few months, not every few years.

2. Establish Clear Data Governance Boundaries

Set the rule before someone has to guess it in the moment. A simple two-tier standard is enough to start:

! REQUIRES REVIEW BEFORE USE

- Client names, contracts, or case details
- Financial statements or projections
- Employee records or personal information
- Source code, trade secrets, or proprietary processes
- Anything covered by an NDA or regulatory obligation

✓ GENERALLY SAFE FOR STAFF USE

- Publicly available information
- Properly anonymized or aggregated data
- General research and first-draft writing
- Internal brainstorming with no identifying details

3. Vet AI Tools Like Any Other Vendor

Before approving a tool for company-wide use, ask the same questions you'd ask of any vendor handling business data:

- Where is our data stored, and for how long?
- Is our data used to train the vendor's models?
- Does the vendor carry SOC 2 (or equivalent) certification?
- Can we get an enterprise agreement with admin controls and audit logs?
- Who internally can grant or revoke access?

REMEMBER

Free, personal-tier AI accounts almost always reserve the right to use your inputs to train their models. An enterprise or business-tier agreement is the difference between "we tried a chatbot" and "we made a defensible business decision."

4. Put the Policy in Writing, and Assign an Owner

A one-page AI usage policy beats an unwritten understanding every time. At minimum, it should cover approved tools, data classification rules, required disclosures, and who to ask when a use case isn't covered.

REMEMBER

A policy nobody owns is a policy nobody follows. Assign it to a specific person or role — not "the team."

5. Plan for Oversight, Not Just Adoption

Approving AI tools is the easy part. The businesses that avoid trouble are the ones that keep watching after rollout:

! UNGOVERNED AI USE

- Shadow AI tools nobody signed off on
- No record of what data went where
- Incidents discovered after the fact, if at all
- Liability with no paper trail to point to

✓ GOVERNED AI USE

- An approved tool list staff actually use
- Regular training on what's safe to share
- A clear path to report a mistake early
- Documentation your insurer or regulator can review

Questions or Concerns?

If you need help selecting secure, enterprise-ready AI tools that keep your data private, reach out to us. We can review what your team is already using, close the gaps, and help you put a policy in place that fits how your business actually works.

CALL

647.478.8449

EMAIL

info@canopytech.ca

WEBSITE

canopytech.ca