Safe AI Usage Process for SMEs

A simple process to discover AI use, protect sensitive data, switch on existing controls and show clients that AI is being governed properly.

Use this document as a starting point for AI governance, supplier security reviews, cyber insurance assessments, and client due diligence. It forms the foundation of an official AI Usage Policy, with the next step being ongoing governance reviews, approved tool assessments and evidence collection.

The Enable IT AI Data Security Process

The aim is not to block AI. The aim is to make AI use visible, controlled and defensible. Start with the highest-risk data and the smallest number of staff who handle it, then widen the programme over time.

Step	What to do
1. Discover Shadow AI	Map every AI tool touching company or client data, including browser extensions and personal accounts.
2. Classify Data Rules	Define what must never be entered into public AI tools: client contracts, tender pricing, banking details, employee records and confidential IP.
3. Configure Existing Controls	Turn on controls already included in business subscriptions: SSO, MFA, retention settings, training opt-out, audit logs and approved-app access.
4. Approve Vendors	Before approving a new AI tool, confirm hosting location, training use, retention, DPA terms and account ownership.
5. Train High-Risk Users	Start with staff who touch contracts, tenders, finance, HR and client data. Train them on safe prompts, red flags and escalation. Then proceed to train the rest of the staff on safe AI usage.
6. Review Monthly	Review new tools, audit risky activity, remove unused access and update the approved AI list.

Why this matters now

Supply chain requirements and large company procurement processes are increasingly requiring suppliers to demonstrate stronger cyber security and AI governance controls. AI governance is becoming part of the same conversation as Essential Eight maturity, privacy obligations and supplier questionnaires.

Australia's Privacy Act and Australian Privacy Principles already govern personal information. The Privacy and Other Legislation Amendment Act 2024 introduced automated decision-making transparency obligations that commence on 10 December 2026 for applicable entities.