

AI STRATEGY · POLICY

AI Data Handling Policy

Sets out what data can and cannot be shared with AI tools, and how AI-related data risk is managed.

How to use this: Adopt as-is and pair with the Acceptable Use of AI Policy; review annually or whenever a new AI tool category is approved.

Data Classification for AI Use

Not all company data carries the same risk when shared with an AI tool, so classify before deciding what's shareable.

Data type	Examples	Shareable with approved AI tools?
Public	Marketing copy, published docs	Yes
Internal, non-sensitive	Draft internal reports, general product docs	Yes, with approved tools only
Confidential	Financials, unreleased product plans, contracts	Only with tools specifically approved for this tier
Customer / personal data	Customer PII, usage data, support ticket content	Only with tools under a signed data processing agreement

Rules for AI Tool Data Handling

- ☐ No customer personal data is entered into any AI tool without a reviewed data processing agreement in place
- ☐ No credentials, API keys, or secrets are ever entered into an AI tool, approved or otherwise
- ☐ Confidential company data is only used with tools explicitly approved for that classification tier
- ☐ Default assumption for any new, unapproved tool is that no company data may be entered

Vendor and Retention Considerations

Who reviews an AI vendor's data retention and training-use terms before approval?

What is our policy on AI vendors using our data to train their models (default: opt out where possible)?

How often is the approved tools list reviewed against updated vendor terms?
