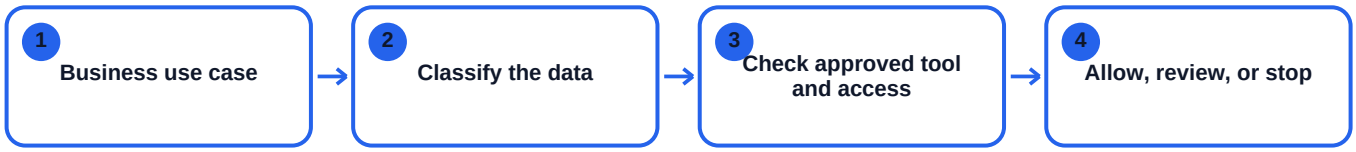
PRIVATE GPT WORKING RESOURCE

AI Data Handling Policy Workbook

Turn an AI policy into enforceable rules for tools, data classes, access, retention, review, and incident response.



Define your operating rules

Policy owner and approval date	
Approved-tool register owner	
Data-classification source of truth	
Prohibited data and secrets	
Retention and logging reviewer	
Incident reporting channel	

Decision notes

PRIVATE GPT LAUNCH GATE

Readiness checklist

Attach a written rule, owner, or test result to every checked line. A blank answer is a reason to keep that path out of the first launch.

- [ ] Inventory the AI tools, accounts, extensions, and meeting bots already in use.
- [ ] Name the approved business use cases for each tool rather than approving a tool for every purpose.
- [ ] Map public, internal, confidential, regulated, privileged, and contract-restricted data to explicit rules.
- [ ] Prohibit passwords, private keys, access tokens, and other secrets in conversational AI interfaces.
- [ ] Require approved company accounts and define who grants, reviews, and removes access.
- [ ] Document retention, deletion, logging, vendor use, and model-training controls for each environment.
- [ ] Require qualified human review before consequential, external, or sensitive output is used.
- [ ] Define the stop-work and reporting path for restricted data, suspicious output, or unauthorized access.
- [ ] Train employees with examples from their actual work and provide a safe path for questions.
- [ ] Set a review trigger for new tools, contracts, regulations, incidents, and material use-case changes.

Test scenarios

[ ] Public content Result / owner: _____	[ ] Client-confidential data Result / owner: _____	[ ] Personal AI account Result / owner: _____
[ ] Consequential output Result / owner: _____	[ ] Accidental restricted data Result / owner: _____	[ ] Departing employee Result / owner: _____

Ready to scope the workflow? Book a meeting at https://getprivategpt.com/contact. We will review the operating rules first, then discuss scope and pricing.