KeenBench Security & Data Handling (Fictional QA)

KeenBench - Security & Data Handling Notes (Fictional QA Data)

QA marker: KEENBENCH_SECURITY_DOC=V1

Principles

- Explicit egress consent before sending any Workbench content to a model provider.

- Draft-first writes: model output may propose changes, but the user reviews diffs before publishing.

- Local-first review: diffing and review UI must not trigger model calls.

Data handling

- API keys are stored locally and encrypted at rest.

- Workbench files may include sensitive business information; treat all inputs as confidential by default.

What to avoid (in docs and UI copy)

- Do not imply we train on customer data.

- Do not claim guarantees we cannot verify.