Evaluate security and trust

Use the public controls and evidence boundaries to assess the platform without relying on marketing shorthand.

Task: Complete an initial security, privacy and responsible-AI review.

Audience: Security reviewers, data protection leads and practice principals

Owner: Obedience Security

Version 2026.08 | Reviewed 2026-08-13 | Next review 2026-10-13

Review the boundary

- Read the security, privacy, responsible-AI and subprocessor policies from the governed policy hub.
- Use the data-location wording as written. Do not infer that every supporting provider stores data in the United Kingdom.
- Treat an external penetration review as separate evidence from internal tests and application gates.

Report a vulnerability

Follow the vulnerability disclosure policy. Do not access another customer's data, create avoidable availability impact or publish a live weakness before coordinated review.

Ask for evidence

Procurement and security teams can request a bounded evidence pack. Restricted architecture, infrastructure and incident material is shared only after identity and purpose checks.