Xelora Ai — Security & Trust Overview

This overview describes the current security model of Xelora Ai during the Operations Pilot.

Access & Identity

• Single Sign-On (Google, Microsoft) on the roadmap
• Email / password with strong password rules today
• Role-based access control: Admin, Manager, Member, Client
• Per-workspace permission scoping

Data Isolation

• Each Client Brain is logically isolated
• Queries scoped to workspace; no cross-client leakage
• Internal vs external visibility flags per document

Auditability

• Audit logs of who asked what and what an agent did
• Source citations on every AI answer
• Approval Center for sensitive actions and outbound content

Infrastructure

• Hosted on managed, SOC 2 Type II compliant cloud providers
• TLS 1.2+ in transit, AES-256 at rest
• Daily backups with point-in-time recovery

Roadmap

• SSO / SAML
• SCIM provisioning
• Customer-managed encryption keys
• Private/local deployment
• SOC 2 Type II report (in progress)

Disclaimer

• Xelora Ai is an early-stage product. Formal certifications (SOC 2, HIPAA) are not yet completed. Contact security@xeloraai.com for the latest status.