Security and compliance posture.

If you're reviewing Bildstak for IT or procurement, this is your reference: certifications, encryption, access control, data residency, and deployment modes, with a downloadable one-pager.

Compliance at a glance

SOC 2 Type I	Target Q4 2026
SOC 2 Type II	In progress
ISO 27001	Planned, Year 3
GDPR	Aligned by design
PIPEDA	Aligned for Canadian customers
HIPAA	Friendly via BYO-LLM-key and customer-side data on private deployments
Annual penetration test	Yes

Authentication

JWT on every request. Email and password with verification. Google OAuth. SAML and OIDC for enterprise SSO. Per-visitor JWT for embedded surfaces.

Authorization

Project-level RBAC (Owner, Admin, Editor, Viewer). AST-level SQL scope rewriter (built on sqlglot) injects per-tenant WHERE clauses into every query. Three-layer defense: customer middleware, source-level allowlist, AST rewriter. An LLM bug, an SQL injection attempt, or a rule misconfiguration each get caught by another layer.

Encryption

Fernet symmetric encryption for credentials at rest. TLS 1.2+ in transit. JWT secrets encrypted at rest. Master key in environment variable, managed via cloud KMS.

Data residency

- Canada: AWS Canada Central, Montréal
- European Union: Hetzner Helsinki
- Customer-VPC for those who require it
- Air-gapped on-premises for classified and defence

Logging and audit

Every executed SQL recorded with user, tenant, SQL hash, latency, status, token usage. Every ERP writeback journalled with full request and response bodies. Project audit log of every membership change, source addition, and conversation creation. Auditor read-only share links available for compliance reviews.

Retention

Active customer data retained while contract is active. Departed customer data: 90 days then hard delete. Audit logs: 7 years. Backups: 30 days.