Enterprise Security Posture

Prepared for procurement and security teams

INFRASTRUCTURE

- All services hosted on Microsoft Azure with SOC 2 Type II, ISO 27001, and FedRAMP certifications
- Azure Container Apps with managed TLS, WAF, and DDoS protection via Azure Front Door
- Secrets stored exclusively in Azure Key Vault with RBAC access control and rotation policies
- Infrastructure defined in code (Bicep/Terraform) — no manual portal configuration in production

APPLICATION SECURITY

- Multi-tenant architecture with mandatory tenant isolation at database query level
- Azure AD / Entra ID authentication with RBAC and least-privilege access
- All API endpoints require valid bearer tokens with role-based authorization
- Input validation at all system boundaries, parameterized queries via Entity Framework Core
- HTTPS everywhere with HSTS, CSP headers, and CORS allowlists (no wildcard origins)

DATA HANDLING

- Customer data encrypted at rest (AES-256) and in transit (TLS 1.3)
- PII fields identified in data model — data retention policies enforced
- No PII transmitted to third-party AI services — only operational metrics
- Audit logging on all admin actions and PII-containing endpoint access

DEVELOPMENT PRACTICES

- CI/CD pipelines with automated test suites, static analysis, and dependency vulnerability scanning
- Conventional commit format with PR review required — no direct pushes to production branches
- Dependency audit (npm audit / dotnet list --vulnerable) runs in CI pipeline
- Major dependency versions pinned; automated minor/patch updates via Dependabot

INCIDENT RESPONSE

- 24-hour acknowledgement SLA for security incidents reported to security@thelobbi.io
- Structured incident response process: detect, contain, eradicate, recover, postmortem
- Application Insights monitoring with anomaly alerts and structured JSON logging