Compliance Readiness Checklist

Prepared for procurement and security teams

VENDOR DUE DILIGENCE

- Cloud hosting on SOC 2 / ISO 27001 certified infrastructure (Microsoft Azure)
- No customer data shared with sub-processors without explicit disclosure
- Business continuity and disaster recovery plan documented and tested
- Insurance: professional liability / E&O coverage maintained

DATA PROTECTION

- Encryption at rest (AES-256) and in transit (TLS 1.3) for all customer data
- Multi-tenant isolation enforced at database query level — no cross-tenant data access
- Right-to-deletion supported — customer data can be fully purged on request
- PII fields identified and classified in data model documentation

ACCESS CONTROL

- Identity via Azure AD / Entra ID — no local credential stores
- Role-based access control (RBAC) with least-privilege defaults
- Admin actions require elevated roles and produce audit log entries
- Service-to-service auth via managed identities — no shared secrets in code

DELIVERY & CHANGE MANAGEMENT

- All infrastructure changes through code — no manual portal edits in production
- CI/CD pipelines with automated tests, security scanning, and PR review gates
- Blue/green deployments with traffic splitting for production rollouts
- Rollback capability documented and tested for every production deployment

ENGAGEMENT STRUCTURE

- Fixed-scope pricing — deliverables, timeline, and cost agreed before work starts
- Zero lock-in — cancel any time with no penalty, full data export available
- Client owns all custom code and IP produced during engagement
- Managed infrastructure option — The Lobbi hosts, monitors, and maintains