SECURITY & COMPLIANCE STANDARDS

Enterprise Data Security Architecture & Audit Posture

1. PERIMETER DEFENSE AND AUTHENTICATION IDENTITY

Candelas AI Development LLC enforces a zero-trust network access model across all client interfaces. User authentication is secured via a stateful JSON Web Token (JWT) architecture. Tokens are signed using cryptographic keys and stored inside HTTP-only, secure, same-site cookie wrappers, completely neutralizing cross-site scripting (XSS) and cross-site request forgery (CSRF) attack vectors.

2. RATE-LIMITING AND SENTINEL TRAFFIC GATING

To defend against denial-of-service (DoS) attempts and programmatic API abuse, our ingress edge routers deploy strict rate-limiting sentinel rules. Traffic spikes are dynamically evaluated at the network boundary; any unauthorized IP signature breaching standard transaction limits triggers an automatic, temporary lockout response.

3. STORAGE ARCHITECTURE AND FINANCIAL COMPLIANCE

All structured enterprise databases are built with logical row-level isolation to prevent cross-tenant leakage. Furthermore, our financial processing layers mandate strict B2B wire transaction audits, confirming routing parameters against corporate ledgers before unlocking administrative write operations.

4. GLOBAL REGULATORY COMPLIANCE PROFILE

Our platform architecture is mapped directly against major global regulatory compliance standards to guarantee the safety of enterprise data assets:

- **ISO/IEC 27001:2022:** Our core operating framework enforces strict information security management system (ISMS) controls across all cloud boundaries.
- **SOC 2 Type II:** Our infrastructure undergoes regular testing against trust services criteria covering security, availability, and processing integrity.

- **HIPAA Security Rule:** For healthcare integrations, we implement full transport encryption, granular role-based access controls, and customer-managed encryption keys (CMEK) via Google Cloud KMS to protect ePHI.

5. SALES TEAM AUDIT SUPPORT & CONTACT GUIDANCE

To help our clients avoid the overhead of costly, redundant third-party security audits during procurement cycles, Candelas AI Development maintains a pre-compiled **Compliance Assessment Packet**. This packet includes our active system architecture diagrams, bridge letters, and third-party penetration testing summaries.

Your sales and procurement teams can request access to this compliance documentation by contacting our corporate operations desk directly at:

> **Candelas AI Compliance Operations Group**
> Secure Intake Portal: `compliance@candelasai.com`
> Reference Token: `CAID-AUDIT-REDUCTION-2026`

APPENDIX: ACCREDITED REGULATORY SOURCES

American Institute of Certified Public Accountants. (2020). *Trust services criteria for security, availability, processing integrity, confidentiality, and privacy* (SERS No. 1). https://www.aicpa.org

Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. §§ 164.302-164.318 (2013). https://www.hhs.gov/hipaa

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org