Security & Compliance Whitepaper

Enterprise-Grade Data Protection for AI-Powered Solutions

CohrenzAI

Noida, Uttar Pradesh, India

info@cohrenzai.com | +91 8273597975

Confidential - For Authorized Use Only

1. Executive Summary

At CohrenzAI, security is not an afterthought -- it is foundational to everything we build. This whitepaper provides a comprehensive overview of our security architecture, data protection practices, compliance measures, and the safeguards we implement to protect our clients' data and their end-users' information.

As an AI-powered platform that processes sensitive business data and customer conversations, we understand the critical importance of maintaining the highest security standards. Our security framework is designed to meet enterprise requirements while enabling the seamless, simple integration experience our clients expect.

2. Security Architecture

2.1 Defense-in-Depth Approach

CohrenzAI implements a defense-in-depth security strategy with multiple layers of protection:

- Network Layer: TLS 1.2+ encryption for all data in transit, firewall protection, and DDoS mitigation
- Application Layer: Input validation, CORS policies, API key authentication, and rate limiting
- Data Layer: Encrypted storage at rest, parameterized SQL queries, and access controls
- Infrastructure Layer: Cloud security controls, regular patching, and vulnerability management

2.2 Authentication & Authorization

CohrenzAI uses a multi-tier authentication system:

- API Key Authentication: Every chatbot deployment requires a valid API key for backend communication
- Public Key Verification: Client-side script tags include a public key for request verification
- Session Management: Unique cryptographic session IDs generated per conversation with format: session_{timestamp}_{random_alphanumeric}
- Environment Variable Security: All credentials, API keys, and secrets are stored securely in environment variables, never hardcoded

2.3 Cross-Origin Resource Sharing (CORS)

Our FastAPI middleware implements configurable CORS policies that restrict which domains can interact with the CohrenzAI API. In production deployments, CORS is locked down to only authorized client domains, preventing unauthorized access from unknown origins.

3. Data Protection

3.1 Data Classification

We classify data into four categories with appropriate security controls for each:

- Public: Marketing content, website information, public documentation
- Internal: Platform metrics, aggregated analytics, system configurations
- Confidential: Business Data (PDFs, documents), conversation logs, lead information
- Restricted: API keys, database credentials, encryption keys, authentication tokens

3.2 Data Encryption

- In Transit: All API communications use HTTPS with TLS 1.2+ encryption. No plaintext data transmission is permitted.
- At Rest: Database storage uses encrypted volumes. FAISS indexes containing document embeddings are stored on encrypted filesystems.
- Key Management: Encryption keys are managed through secure key management practices with regular key rotation schedules.

3.3 Data Isolation

Each client's data is logically isolated within our platform:

- Separate FAISS indexes per client for document embeddings
- Session-based conversation isolation preventing cross-session data leakage
- Client-specific API keys ensuring requests are routed to correct knowledge bases
- Database-level access controls for lead and conversation data

3.4 Data Retention & Deletion

- Active accounts: Data retained as long as the account is active
- Account termination: 30-day grace period for data export, followed by permanent deletion
- Conversation logs: Retained per client configuration and applicable legal requirements
- Right to deletion: Clients can request complete data deletion at any time

4. Application Security

4.1 Secure Coding Practices

- Input Validation: Pydantic models enforce strict type checking and validation on all API inputs

- SQL Injection Prevention: All database queries use parameterized prepared statements -- no string concatenation in SQL queries
- Output Encoding: AI-generated responses are sanitized before delivery to prevent XSS attacks
- Error Handling: Secure error handling that prevents information leakage in error responses
- Dependency Management: Regular updates of all third-party libraries and dependencies

4.2 AI-Specific Security

- Prompt Injection Protection: Our prompt templates are structured to prevent prompt injection attacks
- Context Boundaries: AI responses are constrained to provided business context -- the chatbot cannot access or reveal system prompts, internal configurations, or data from other clients
- Response Filtering: AI outputs are monitored for potentially harmful, inappropriate, or off-topic content
- Model Security: We use Azure OpenAI's enterprise-grade AI services with Microsoft's built-in content safety filters

5. Infrastructure Security

5.1 Cloud Security

- Hosted on enterprise-grade cloud infrastructure with ISO 27001 certification
- Network segmentation and virtual private cloud isolation
- Automated security patching and update management
- Regular penetration testing and vulnerability assessments
- 24/7 infrastructure monitoring with automated alerting

5.2 Deployment Security

- Docker containerization for consistent, isolated deployments
- Gunicorn + Uvicorn production server with worker process isolation
- Environment-specific configurations preventing development secrets from reaching production
- CI/CD pipeline with automated security scanning

6. Compliance Framework

6.1 Indian Data Protection Laws

CohrenzAI complies with the Digital Personal Data Protection Act (DPDPA) 2023 and related Indian data protection regulations. We implement:

- Lawful purpose limitation for data processing
- Data minimization -- collecting only necessary information
- Purpose limitation -- using data only for stated purposes
- Storage limitation -- retaining data only as long as needed
- Data breach notification within 72 hours

6.2 International Standards

Our security practices align with international frameworks including:

- ISO 27001 principles for information security management
- SOC 2 Type II principles for security, availability, and confidentiality
- GDPR principles for clients serving European customers
- OWASP Top 10 mitigation for web application security

6.3 Industry-Specific Compliance

We support industry-specific compliance requirements:

- Healthcare: Architecture designed to support HIPAA requirements for patient data
- Financial Services: Controls aligned with RBI guidelines for customer data protection
- E-Commerce: PCI DSS awareness for payment-adjacent data handling

7. Incident Response

7.1 Response Plan

CohrenzAI maintains a formal incident response plan:

- Detection: 24/7 monitoring with automated threat detection
- Containment: Immediate isolation of affected systems
- Eradication: Root cause analysis and threat elimination
- Recovery: Systematic restoration from verified backups
- Post-Incident Review: Lessons learned and security improvements

7.2 Notification

Affected clients are notified within 72 hours of confirmed data breaches, with full transparency about the scope, impact, and remediation steps taken.

8. Business Continuity

- Regular automated backups of all databases and knowledge bases
- Multi-region infrastructure for geographic redundancy
- Disaster recovery procedures with defined RTO and RPO objectives
- Regular backup restoration testing to ensure data recoverability

9. Contact Security Team

For security concerns, vulnerability reports, or compliance inquiries:

- Security Email: info@cohrenzai.com
- Phone: +91 8273597975
- Responsible Disclosure: We welcome responsible security vulnerability reports