Security and Compliance in Aimyze

Version 1.0 | December 2025

1. Security Overview

Aimyze is built with enterprise-grade security at its core. This document outlines our security architecture, compliance commitments, and the measures we take to protect your data and operations.

Security is not an afterthought at Aimyze - it is foundational to every aspect of our platform design, development, and operations.

2. Data Security

2.1 Encryption

Data at Rest: All customer data is encrypted using AES-256 encryption. Encryption keys are managed through AWS Key Management Service (KMS) with customer-managed key options for Enterprise tier.

Data in Transit: All network communications are encrypted using TLS 1.3. We enforce HTTPS for all API endpoints and web interfaces.

Database Encryption: Database-level encryption is enabled for all data stores, including transparent data encryption (TDE) for relational databases.

2.2 Data Residency

Customer data is stored in AWS Mumbai region (ap-south-1), ensuring:

- Compliance with Indian data localization requirements
- Low-latency access for India-based operations
- Alignment with Digital Personal Data Protection Act requirements

2.3 Data Isolation

Multi-tenant data isolation is enforced through:

- Logical separation at the application layer
- Tenant-specific encryption keys
- Database-level row security policies
- Network isolation using VPC and security groups

3. Access Control

3.1 Authentication

- Single Sign-On (SSO) support via SAML 2.0 and OpenID Connect
- Multi-Factor Authentication (MFA) enforcement
- Password policies aligned with NIST guidelines
- Session management with configurable timeout policies

3.2 Authorization

- Role-Based Access Control (RBAC) with predefined roles
- Granular permissions at feature and data level
- Principle of least privilege enforced
- Regular access reviews and certification

4. Infrastructure Security

4.1 Network Security

- Virtual Private Cloud (VPC) isolation
- Web Application Firewall (WAF) protection
- DDoS protection via AWS Shield
- Private connectivity options (AWS PrivateLink, VPN)
- IP whitelisting capabilities

4.2 Application Security

- Secure software development lifecycle (SSDLC)
- Regular vulnerability scanning and penetration testing
- Dependency scanning and management
- Code review requirements for all changes
- Automated security testing in CI/CD pipeline

5. Compliance & Certifications

5.1 Current Status

Aimyze maintains the following compliance posture:

- DPDP Act (India): Aligned with Digital Personal Data Protection Act 2023 requirements
- IT Act 2000: Compliant with Information Technology Act provisions
- GDPR Readiness: Data processing practices aligned with GDPR principles

5.2 Certifications in Progress

We are actively pursuing the following certifications:

- ISO 27001: Information Security Management System certification
- SOC 2 Type II: Service Organization Control audit
- ISO 27701: Privacy Information Management System

Expected completion timelines are available upon request.

6. Security Operations

6.1 Monitoring & Logging

- 24/7 security monitoring and alerting
- Comprehensive audit logging of all system activities
- Log retention for compliance requirements
- SIEM integration for security event correlation

6.2 Incident Response

Our incident response process includes:

- Documented incident response procedures
- Dedicated security incident response team
- Customer notification within 72 hours for data breaches affecting customer data
- Post-incident analysis and remediation

7. Security Audit Rights

Enterprise customers may request:

- Security questionnaire completion (SIG, CAIQ, or custom)
- Penetration test reports (upon NDA)
- SOC 2 reports (when available)
- Third-party security audit with reasonable notice and at customer's expense

8. Business Continuity

8.1 Availability

- 99.9% uptime SLA commitment
- Multi-AZ deployment for high availability
- Automated failover capabilities
- Regular disaster recovery testing

8.2 Backup & Recovery

- Daily automated backups
- Point-in-time recovery capability
- Geographically distributed backup storage
- Documented recovery procedures

9. Contact

For security inquiries:

Security Team: security@aimyze.com

Report Vulnerabilities: security@aimyze.com