Security Guide

Best Practices for Secure AI Agent Deployment and Data Protection

Version 1.0 | December 2025

1. Introduction

This Security Guide provides comprehensive best practices for deploying Aimyze AI agents securely within your enterprise environment. Following these guidelines will help ensure data protection, maintain compliance, and minimize security risks.

Security is a shared responsibility. While Aimyze implements robust security measures at the platform level, customers play a critical role in securing their environment, access controls, and data handling practices.

2. Shared Responsibility Model

Understanding the security responsibilities between Aimyze and customers is essential:

2.1 Aimyze Responsibilities

- Platform infrastructure security and hardening
- Data encryption at rest and in transit
- Application security and vulnerability management
- Security monitoring and incident response
- Compliance certifications and audits
- Secure software development practices
- Regular security updates and patches

2.2 Customer Responsibilities

- User access management and authentication
- Network security and firewall configuration
- Secure credential management for integrations
- Data classification and handling policies
- Employee security awareness training
- Incident reporting and coordination
- Compliance with applicable regulations

3. Pre-Deployment Security Checklist

Before deploying Aimyze agents, complete the following security preparations:

3.1 Access & Identity

- Identify all users who will access the Aimyze platform
- Define role-based access control (RBAC) requirements
- Configure Single Sign-On (SSO) if using enterprise identity provider
- Enable Multi-Factor Authentication (MFA) for all users
- Document access approval and revocation procedures

3.2 Network Security

- Identify network paths between Aimyze and your systems
- Configure firewall rules to allow only required traffic
- Set up VPN or private connectivity for sensitive integrations
- Implement IP whitelisting where supported
- Document network architecture and data flows

3.3 Integration Security

- Create dedicated service accounts for Aimyze integrations
- Apply principle of least privilege to all credentials
- Store credentials securely (never in plain text or code)
- Establish credential rotation schedule
- Document all integration touchpoints and permissions

3.4 Data Classification

- Identify data types that will be processed by agents
- Classify data according to sensitivity levels
- Ensure compliance with data handling policies
- Document data retention requirements
- Identify any data that should be excluded from processing

4. Access Control Best Practices

4.1 User Authentication

Enable SSO: Integrate with your enterprise identity provider (Okta, Azure AD, etc.) for centralized authentication and consistent security policies.

Enforce MFA: Require multi-factor authentication for all users, especially administrators and those with access to sensitive data.

Password Policies: If not using SSO, enforce strong password requirements: minimum 12 characters, complexity requirements, and regular rotation.

Session Management: Configure appropriate session timeouts based on data sensitivity. Shorter timeouts for administrative access.

4.2 Role-Based Access Control

Implement granular access control using Aimyze's RBAC features:

Administrator: Full platform access. Limit to essential personnel only.

Operator: Day-to-day operations, alert management, reporting. Standard user role.

Viewer: Read-only access to dashboards and reports. Use for stakeholders needing visibility.

API User: Programmatic access only. Use for system integrations.

Review and certify access rights quarterly. Remove access immediately upon role change or departure.

4.3 Service Account Security

For integration service accounts:

- Create unique service accounts for each integration
- Never share service accounts between systems
- Grant minimum permissions required for functionality
- Disable interactive login for service accounts
- Monitor service account activity for anomalies
- Rotate credentials every 90 days (minimum)

5. Network Security Best Practices

5.1 Secure Connectivity

Choose the appropriate connectivity option based on your security requirements:

Public Internet (HTTPS): Suitable for low-sensitivity deployments. All traffic encrypted via TLS 1.3.

VPN: Recommended for standard enterprise deployments. Provides encrypted tunnel between your network and Aimyze.

AWS PrivateLink: Recommended for high-security deployments. Traffic never traverses public internet.

5.2 Firewall Configuration

Configure your firewall to:

- Allow outbound HTTPS (443) to Aimyze endpoints
- Restrict inbound traffic to only required webhook callbacks
- Block all unnecessary ports and protocols

- Log all traffic for security monitoring
- Review firewall rules quarterly

5.3 IP Whitelisting

For additional security:

- Whitelist Aimyze IP ranges in your systems (provided during onboarding)
- Configure Aimyze to accept connections only from your IP ranges
- Update whitelist when network changes occur

6. Data Protection Best Practices

6.1 Data Minimization

Reduce risk by limiting data exposure:

- Only share data necessary for agent functionality
- Mask or redact sensitive fields not required for processing
- Avoid including personal data unless essential
- Regularly review data being shared with agents

6.2 Sensitive Data Handling

For data requiring special protection:

- Identify PII, financial data, health information, and trade secrets
- Apply additional access controls for sensitive data
- Consider data anonymization or pseudonymization
- Ensure compliance with applicable regulations (DPDP, GDPR, etc.)
- Document handling procedures and train relevant personnel

6.3 Data Retention

Implement appropriate retention practices:

- Define retention periods based on business and legal requirements
- Configure agent data retention settings accordingly
- Implement secure data deletion procedures
- Document retention policies and exceptions

7. Operational Security

7.1 Change Management

Implement controls for configuration changes:

- Require approval for significant configuration changes
- Test changes in non-production environment first
- Document all changes with business justification

- Maintain rollback procedures
- Review changes during security audits

7.2 Monitoring & Alerting

Establish security monitoring:

- Enable audit logging for all user and agent activities
- Configure alerts for security-relevant events
- Monitor for unusual access patterns or data volumes
- Integrate Aimyze logs with your SIEM if available
- Review logs regularly for anomalies

7.3 Security-Relevant Events to Monitor

- Failed login attempts (especially multiple failures)
- Access from new locations or devices
- Bulk data exports or unusual data access
- Administrative configuration changes
- Integration connection failures
- Agent actions outside normal patterns

8. Incident Response

8.1 Preparing for Incidents

Be prepared to respond to security incidents:

- Document incident response procedures specific to Aimyze
- Identify incident response team and contact information
- Know how to disable agent actions quickly if needed
- Maintain Aimyze support contact information
- Test incident response procedures periodically

8.2 Reporting Security Incidents

If you suspect a security incident involving Aimyze:

1. Immediately contact Aimyze Security: security@aimyze.com
2. Provide details: what happened, when, what systems affected
3. Preserve evidence: do not delete logs or make unnecessary changes
4. Coordinate response actions with Aimyze team
5. Document all actions taken

8.3 Aimyze Incident Notification

Aimyze will notify customers of security incidents affecting their data within 72 hours. Notifications will include:

- Nature and scope of the incident

- Data potentially affected
- Actions taken by Aimyze
- Recommended customer actions
- Point of contact for updates

9. Compliance Considerations

9.1 Regulatory Compliance

Ensure your Aimyze deployment meets regulatory requirements:

DPDP Act (India): Implement appropriate consent mechanisms, data localization (Aimyze stores data in India), and data subject rights procedures.

Industry Regulations: Consider sector-specific requirements (e.g., RBI guidelines for financial services, HIPAA considerations for healthcare data).

Internal Policies: Align Aimyze usage with your organization's security and privacy policies.

9.2 Audit Readiness

Maintain audit-ready documentation:

- Access control policies and user lists
- Integration inventory with permissions
- Data flow documentation
- Security configuration settings
- Incident response procedures
- Audit logs and retention records

10. Security Review Cadence

Maintain ongoing security hygiene with regular reviews:

10.1 Weekly

- Review security alerts and incidents
- Check integration health and connectivity
- Monitor agent activity for anomalies

10.2 Monthly

- Review user access and permissions
- Check for unused or orphaned accounts
- Review audit logs for anomalies
- Verify backup and recovery procedures

10.3 Quarterly

- Conduct access certification review
- Review and update security documentation
- Rotate service account credentials
- Review firewall rules and network configuration
- Assess compliance with security policies

10.4 Annually

- Comprehensive security assessment
- Review and update incident response procedures
- Evaluate new security features and options
- Conduct security awareness training refresh

11. Security Resources

11.1 Aimyze Security Contacts

Security Team: security@aimyze.com

Report Vulnerabilities: security@aimyze.com

Privacy Inquiries: privacy@aimyze.com

Support: support@aimyze.com

11.2 Documentation

- Security and Compliance Document: Aimyze security architecture and compliance posture
- Privacy Policy: Data handling and privacy practices
- Terms and Conditions: Legal terms including security obligations
- API Reference: Secure API usage guidelines

11.3 Security Questionnaires

Aimyze can provide completed security questionnaires upon request:

- SIG (Standard Information Gathering)
- CAIQ (Consensus Assessments Initiative Questionnaire)
- Custom questionnaires (reasonable scope)

Contact your account manager or security@aimyze.com to request.

12. Summary: Security Checklist

Quick reference checklist for secure deployment:

- SSO/MFA enabled for all users
- RBAC configured with least privilege
- Service accounts created with minimal permissions
- Credential rotation schedule established
- Network connectivity secured (VPN/PrivateLink if required)
- Firewall rules configured
- IP whitelisting enabled (if applicable)
- Data classification completed
- Sensitive data handling procedures documented
- Audit logging enabled
- Security monitoring configured
- Incident response procedures documented
- Security review cadence established
- Compliance requirements addressed

— End of Security Guide —

Aimyze Software Private Limited
Unit 101, Oxford Towers, 139, HAL Old Airport Rd, Kodihalli, Bengaluru, Karnataka 560008