

Infrastructure

Overview

AIVA is built on modern cloud infrastructure designed to provide secure, scalable, and resilient services. Our infrastructure combines cloud-native security controls, redundant deployment architecture, identity management, continuous monitoring, and documented operational procedures to protect customer data and maintain platform availability.

Cloud Platform

AIVA is hosted using enterprise cloud infrastructure to provide secure and reliable services.

The following cloud platforms and services are in use:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Nebius

These providers support infrastructure, compute, storage, networking, authentication, artificial intelligence services, and platform resiliency.

Infrastructure Architecture

AIVA uses a cloud-native architecture designed around security and operational resilience.

Key architectural principles include:

- Environment segregation
- Least-privilege access
- Redundant infrastructure
- Cloud-native identity services
- Layered network security
- Infrastructure monitoring
- Automated recovery processes

The production environment is physically separated from development and testing environments to reduce operational risk and improve security.

Network Security

Network security controls help protect AIVA against unauthorized access and external threats.

Documented controls include:

- Web Application Firewall (WAF)
- Private networking
- Network segmentation
- Cloud firewalls
- Secure API communications
- TLS 1.2+ encryption

These controls help protect customer traffic while limiting exposure of internal infrastructure.

Identity & Authentication

Administrative and service access is controlled using centralized identity management and authentication services.

Documented controls include:

- AWS Cognito
- OAuth 2.0
- JSON Web Tokens (JWT)
- Multi-Factor Authentication (MFA)
- Role-based authorization
- Least-privilege access

Administrative access is limited to authorized personnel with a legitimate business need.

Production Environment

Production systems are designed to maximize both security and reliability.

Current controls include:

- Physical separation of production from development and testing
- Controlled production deployments
- Documented change management
- Infrastructure monitoring
- Security monitoring
- Audit logging

Changes to production systems follow formal review and approval processes before deployment.

Availability & Resilience

AIVA is designed to maintain service availability through redundant cloud infrastructure and documented operational processes.

Platform resilience includes:

- Multi-availability zone deployment
- Redundant cloud infrastructure
- Automated backups
- Continuous monitoring
- Incident response procedures
- Business continuity planning

These controls help minimize service interruptions and support recovery following operational events.

Monitoring & Logging

Operational visibility is provided through continuous monitoring and centralized logging.

Monitoring includes:

- Infrastructure health
- Platform availability
- Security events
- Administrative activity
- Audit logs
- Operational alerts

Administrative and event logs are retained for a minimum of **180 calendar days**.

Backup & Recovery

Customer data is protected through automated backup processes and resilient cloud infrastructure.

Current capabilities include:

- Automated backups
- Redundant storage locations
- Infrastructure resiliency
- Documented recovery procedures

Capability	Status
Automated Backups	✓
Encrypted Backups	✓
Multiple Backup Locations	✓
Backup Frequency	Daily
Backup Retention	24 hours
Recovery Point Objective (RPO)	TBD
Recovery Time Objective (RTO)	TBD

Change Management

Infrastructure and application changes follow documented change management procedures.

The process includes:

- Risk assessment
- Testing
- Approval workflows
- Deployment validation
- Production acceptance criteria

- Rollback planning where appropriate

Security considerations are incorporated into each stage of the deployment lifecycle.

Business Continuity

AIVA maintains a Business Continuity Program to support the continued operation of AIVA during disruptive events.

The program includes:

- Business impact assessments
- Risk assessments
- Continuity planning
- Recovery procedures
- Regular testing
- Periodic reviews

Business continuity documentation is reviewed and tested on a regular basis.

Disaster Recovery

AIVA incorporates disaster recovery planning as part of its operational resilience strategy.

Current capabilities include:

- Cloud infrastructure redundancy
- Automated backups
- Recovery procedures
- Incident response integration
- Business continuity planning