Security

Overview

Our security program is designed to protect the confidentiality, integrity, and availability of customer data through secure software development, cloud-native security controls, continuous monitoring, and documented operational practices.

Security Program

- Information security governance
- Risk management
- Secure SDLC
- DevSecOps
- Least-privilege access controls
- Vulnerability management
- Incident response
- Annual policy reviews

Our Security Principles

Security is integrated throughout the AIVA platform and software development lifecycle.

Our security program is built around the following principles:

- Secure by Design
- Privacy by Design
- Least Privilege Access
- Defense in Depth
- Continuous Security Validation
- Customer Transparency
- Operational Resilience

These principles guide the development of AIVA as well as the internal security practices used to operate the service.

Secure Software Development

AIVA is developed using a Secure Software Development Lifecycle (Secure SDLC).

Security activities are incorporated throughout development and deployment, including:

- DevSecOps security automation
- Peer code reviews
- Threat modeling
- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Manual penetration testing
- Documented change management
- Production approval processes

All production changes must satisfy documented acceptance criteria before deployment. Security controls are evaluated whenever systems or applications change.

Infrastructure Security

AIVA uses cloud-native security controls to protect customer environments.

Documented infrastructure protections include:

- Web Application Firewall (WAF)
- Private network segmentation
- Cloud firewalls
- Multi-zone environment segregation
- Identity-based access controls
- OAuth2 authentication
- JWT authorization
- AWS Cognito identity management

Production, development, and testing environments are physically segregated to improve security, privacy, and availability.

Identity & Access Management

Access to AIVA systems is governed by documented access control policies.

Security controls include:

- Least privilege access
- Role-based authorization
- Multi-Factor Authentication (MFA)
- Strong password requirements
- Regular access reviews
- Audit logging
- Privileged account management

Internal enterprise systems require MFA, and privileged access is limited to authorized personnel with legitimate business requirements.

Security Monitoring

AIVA continuously monitors operational and security events to support platform reliability and incident detection.

Monitoring includes:

- Operational logs
- Security logs
- Administrator activity logs
- Audit trails
- Infrastructure monitoring
- Availability monitoring

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

Vulnerability Management

AIVA maintains a documented vulnerability management program designed to identify, prioritize, and remediate security issues.

The program includes:

- Routine vulnerability testing
- CVSS-based risk classification
- Patch management
- Manual penetration testing
- Security scanning
- Malware protection

Penetration testing is performed for cloud systems handling customer data, including following significant system changes.

Incident Response

AIVA is designed to support resilient service delivery.

Operational controls include:

- Documented incident response procedures
- Root cause analysis
- Business continuity planning
- Risk assessments
- Redundant cloud infrastructure
- Availability zone failover
- Regular continuity testing

Security incidents are managed through documented procedures that include containment, recovery, investigation, customer notification (where applicable), and continuous improvement.