

RunwaySync Security Overview

Customer Security Brief | Last updated September 10, 2026

RunwaySync is designed to provide airport and FBO teams with a simple, reliable platform while maintaining appropriate safeguards for customer data and system access. Our security practices focus on protecting customer information, limiting administrative access, securing cloud infrastructure, and maintaining recoverability of production systems.

Current assurance status. RunwaySync does not currently maintain a SOC 2 report. We are continuing to formalize our security program using established cloud-security practices and recognized security frameworks as references, and we can provide additional information during customer security reviews.

Cloud Infrastructure

RunwaySync is hosted on Amazon Web Services (AWS). Production and development operate in separate AWS accounts and environments. Centralized AWS administration is managed through a dedicated AWS management account using AWS Organizations and IAM Identity Center.

- Amazon ECS for application workloads
- Amazon RDS for PostgreSQL databases
- Amazon S3 and CloudFront for web application delivery
- AWS-managed networking, security groups, certificates, and related infrastructure services

Administrative Access

Administrative access to RunwaySync's AWS environments is centrally managed through AWS IAM Identity Center.

- Multi-factor authentication for AWS administrative access
- Individual administrative identities rather than shared credentials
- Centralized access management across development and production AWS accounts
- AWS root credentials reserved for root-only or account-recovery functions and not used for routine administration
- Production infrastructure access limited to authorized administrators

Network and Database Security

RunwaySync's production and development PostgreSQL databases are deployed privately within AWS networking environments.

- RDS databases are not publicly accessible
- Database inbound access is restricted through AWS security groups
- Production and development database access is limited to their authorized application infrastructure
- PostgreSQL connections require encrypted TLS connections

Encryption and Secrets

RunwaySync uses HTTPS/TLS to protect application traffic in transit, and PostgreSQL connections are required to use TLS. Production PostgreSQL storage is encrypted at rest using AWS KMS, and production data stored in Amazon S3 uses AWS server-side encryption. Application secrets and sensitive configuration values are managed using AWS services rather than embedded directly within application source code.

Authentication and Authorization

RunwaySync users authenticate using individual application accounts. Passwords are stored using secure one-way password hashing rather than as plaintext credentials. Application authorization uses role-based access controls, with authorization enforced by the backend application.

Access controls are designed to prevent users from performing administrative actions outside their authorized role or accessing resources belonging to another customer organization.

Current limitation: RunwaySync does not currently provide multi-factor authentication for end-user application accounts.

Customer Data Isolation

RunwaySync is a multi-tenant application. Customer access boundaries are enforced by the application authorization layer. Backend authorization has been reviewed to verify that users cannot elevate their own privileges, administer unauthorized organizations, or access another customer's resources by modifying application requests.

Backups and Recovery

Production PostgreSQL data is protected using automated Amazon RDS backups.

- Automated backups with a seven-day retention period
 - Point-in-time recovery capability
 - Successful production database recovery test completed August 18, 2026
- The recovery test validated the ability to restore the production database from backup without modifying the live production environment.

Logging and Monitoring

RunwaySync uses AWS and application-level logging to monitor production operation and investigate issues.

- AWS CloudWatch logging
- Application error and exception monitoring
- Application activity logging for selected security- and operationally relevant events
- Automated alerts for application exceptions and selected operational events

These systems do not represent a guarantee of continuous human monitoring.

Software Development and Change Management

RunwaySync maintains separate development and production environments. Application changes are developed and validated outside the production environment before deployment. Production application workloads are deployed through controlled software deployment processes rather than through direct modification of running production systems. Secrets and environment-specific configuration are kept separate from application source code.

Payment Information

RunwaySync does not directly store complete customer payment-card numbers. Payment processing is handled through Stripe rather than within RunwaySync application databases.

Security Incident Handling

RunwaySync has technical capabilities for identifying, investigating, and responding to application and infrastructure incidents using AWS and application logging. If RunwaySync becomes aware of a suspected security incident affecting its systems or Customer Data, it will take reasonable steps appropriate to the circumstances to investigate, contain and remediate identified risks, and assess impact. RunwaySync is continuing to formalize its written incident-response procedures and supporting security policies as the platform and customer base grow.

Security Assessments and Compliance

RunwaySync does not currently maintain a SOC 2 report and does not represent itself as SOC 2 certified or audited. Our current approach is to maintain practical technical controls appropriate to the platform, verify important controls directly, and provide transparency to customers regarding both implemented protections and areas that continue to mature.

RunwaySync has not yet completed an independent penetration test or SOC 2 examination.

Customers with specific security, compliance, data-handling, or procurement requirements are encouraged to raise those requirements during the evaluation process. RunwaySync can provide additional technical information and participate in reasonable customer security reviews.

Security Contact

Security-related questions, vulnerability reports, customer security questionnaires, or requests for additional technical information may be directed to security@runwaysync.com.

For the most current public security information, visit runwaysync.com/security.

Verified controls as of September 10, 2026: centralized MFA-protected AWS administration; private RDS networking; security-group-restricted database ingress; required PostgreSQL TLS; encrypted production data at rest; backend role-based authorization review; seven-day RDS backups; successful production recovery test.