

RunwaySync Security FAQ

Common security and technology questions for customer, IT, procurement, and vendor-risk reviews.

Security posture at a glance

RunwaySync is hosted on AWS with separated development and production accounts, MFA-protected centralized administration, private RDS databases, TLS-encrypted traffic, encrypted production data at rest, and tested database recovery.

Infrastructure & Hosting

Where is RunwaySync hosted?

RunwaySync is hosted on **Amazon Web Services (AWS)**. Production services use AWS-managed infrastructure including Amazon ECS, Amazon RDS for PostgreSQL, Amazon S3, Amazon CloudFront, and associated AWS networking and security services.

Are development and production separated?

Yes. RunwaySync maintains separate AWS accounts and environments for development and production. Administrative access to both is centrally managed through a dedicated AWS management account using AWS Organizations and IAM Identity Center.

Is the production database publicly accessible?

No. The production PostgreSQL database is hosted on Amazon RDS with public accessibility disabled. Database ingress is restricted through AWS security groups to authorized application infrastructure. The development database is configured similarly.

Are database connections encrypted?

Yes. RunwaySync requires encrypted TLS connections to its PostgreSQL databases. Development and production use PostgreSQL 17 on Amazon RDS with SSL/TLS connections required.

Access & Authentication

Who can access RunwaySync's AWS production environment?

AWS administrative access is limited to authorized administrative identities. Access is centrally managed through **AWS IAM Identity Center** and protected using multi-factor authentication. AWS root credentials are reserved for root-only, recovery, or emergency functions and are not used for routine administration.

Do AWS administrators use multi-factor authentication?

Yes. Administrative AWS access is protected by multi-factor authentication.

Does RunwaySync support multi-factor authentication for application users?

Not currently. RunwaySync users authenticate using individual email and password credentials. End-user MFA is not currently available.

How are passwords stored?

Passwords are not stored in plaintext. RunwaySync uses secure one-way password hashing to store application user passwords.

Does RunwaySync use role-based access controls?

Yes. RunwaySync uses role-based authorization enforced by the backend application. Authorization controls have been reviewed to verify that users cannot elevate their own privileges, perform unauthorized administrative actions, or access another customer's resources by manipulating application requests.

Customer Data

How is customer data separated?

RunwaySync is a multi-tenant application. Customer access boundaries are enforced through backend application authorization. Users are restricted to the organizations, locations, and resources they are authorized to access.

Is customer data encrypted in transit?

Yes. RunwaySync uses HTTPS/TLS for application traffic, and PostgreSQL database connections are required to use TLS.

Is production customer data encrypted at rest?

Yes. Production PostgreSQL storage on Amazon RDS is encrypted using AWS KMS. Data stored in Amazon S3 is protected with AWS server-side encryption (SSE-S3). Sensitive configuration values and credentials stored in AWS Systems Manager Parameter Store use encrypted SecureString parameters.

What customer information does RunwaySync store?

RunwaySync stores information necessary to provide its operational services, which may include user and contact information, aircraft identifiers such as tail numbers, operational records, fueling/service information, and compliance-related records entered by customers.

Does RunwaySync store payment-card information?

No. RunwaySync does not directly store customer payment-card information. Payment-card processing is handled by Stripe, and complete payment-card numbers are not stored in RunwaySync application databases.

Who owns customer data?

Customers retain their ownership rights in the information they submit to RunwaySync. RunwaySync does not sell Customer Data. RunwaySync processes and discloses Customer Data only as permitted by applicable agreements and privacy notices, including as reasonably necessary to provide, secure, maintain, and support the Services. For additional information about permitted data use, see the RunwaySync Privacy Policy and Terms of Service.

Backups & Recovery

Does RunwaySync back up production data?

Yes. The production PostgreSQL database uses automated Amazon RDS backups with a seven-day retention period and point-in-time recovery capability.

Has RunwaySync tested its ability to restore from backup?

Yes. On August 18, 2026, RunwaySync successfully completed a production database recovery test and verified its ability to restore production data from an Amazon RDS backup without modifying the live production environment.

Monitoring & Development

Does RunwaySync maintain system and application logs?

Yes. RunwaySync uses AWS CloudWatch and application-level logging to provide visibility into system operation, errors, authentication activity, selected application changes, and other relevant operational events. Automated alerts are used for application exceptions and selected system events.

How are application secrets managed?

Application secrets and sensitive environment configuration are managed using AWS services rather than embedded directly within application source code. Sensitive values in AWS Systems Manager Parameter Store are stored as encrypted SecureString parameters.

How are software changes deployed?

RunwaySync maintains separate development and production environments. Changes are developed and validated outside production before deployment. Production application workloads are deployed using controlled software deployment processes rather than by directly modifying running production systems.

Security Response & Assessment

Does RunwaySync have an incident-response process?

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 broader security policy framework as the company and platform mature.

Has RunwaySync completed a penetration test?

Not yet. RunwaySync has not currently completed an independent third-party penetration test. Independent security testing is part of the longer-term security maturity roadmap.

Is RunwaySync SOC 2 compliant?

RunwaySync does not currently maintain a SOC 2 report and does not represent itself as SOC 2 certified or audited. RunwaySync is building its security program around practical technical controls and established security practices while using recognized security frameworks, including SOC 2 concepts, as references for continued maturity.

Can RunwaySync complete a customer security questionnaire?

Yes. RunwaySync can provide additional technical information and participate in reasonable security, IT, procurement, and vendor-risk reviews. Customers with specific security or compliance requirements are encouraged to raise those requirements during evaluation so they can be reviewed directly. Security review requests may be sent to security@runwaysync.com.

Questions or security review requests?

Contact security@runwaysync.com for additional technical information, vulnerability reports, or a customer security review.