



# Event Registration Hub

## Security Overview

Platform security, privacy, and operational controls

Version 2026.07 · Generated 11 September 2026

Classification: Public

### **Audience**

Clients, procurement teams, and security reviewers

This document summarizes the security posture of the platform.

## Executive Summary

Event Registration Hub securely manages event registrations, participant data, hotel bookings, payments, transactional emails, and manager access. The platform combines encrypted transport, role-based access control, database-level Row Level Security, two-factor authentication, hosted payment processing, and operational monitoring to protect customer data across its lifecycle.

This document is automatically generated from the current platform configuration and reflects the security controls active on the date shown above.

## Security Highlights

✓ HTTPS / TLS encryption

✓ Role-based access control

✓ Row Level Security (RLS)

✓ Two-factor authentication

✓ Secure hosted payments

✓ Login history & sessions

✓ Account lockout protection

✓ Payment & email logging

## Authentication & Access

|                           |                                           |
|---------------------------|-------------------------------------------|
| Session timeout           | 120 minutes                               |
| 2FA required for admins   | No                                        |
| 2FA required for managers | No                                        |
| Account lockout threshold | 5 failed attempts                         |
| Account lockout duration  | 15 minutes                                |
| Password policy           | min 8 chars, uppercase, lowercase, number |
| Login history             | Enabled                                   |
| Active session tracking   | Enabled                                   |

- Authentication is powered by managed identity with JWT-based sessions.
- TOTP authenticator apps (Google Authenticator, Microsoft Authenticator) are supported. TOTP secrets are encrypted at rest using AES-256-GCM.
- Administrators can enforce 2FA for admin and manager roles.
- Users can review active sessions and revoke individual sessions from Settings.

## Data Protection

- HTTPS/TLS encryption for all data in transit.
- Managed PostgreSQL database with encryption at rest.
- Row Level Security (RLS) policies enforced on application tables.

- Role-based access control across admin, manager, and end-user roles.
- Managers only access the forms and registrations for events assigned to them.
- Privileged service credentials are used only server-side and never shipped to the browser.

## Payment Security

|                          |                                     |
|--------------------------|-------------------------------------|
| <b>Payment provider</b>  | Pelec card (hosted checkout)        |
| <b>Card data storage</b> | Never stored on the platform        |
| <b>Checkout model</b>    | Hosted checkout (redirect / iframe) |

- All card entry happens through the hosted payment provider.
- Payment results are verified server-side before a registration is marked paid.
- Payment transactions, receipts, and sync logs are stored securely and restricted to admins.
- Payment gateway credentials are never exposed to managers or public users.

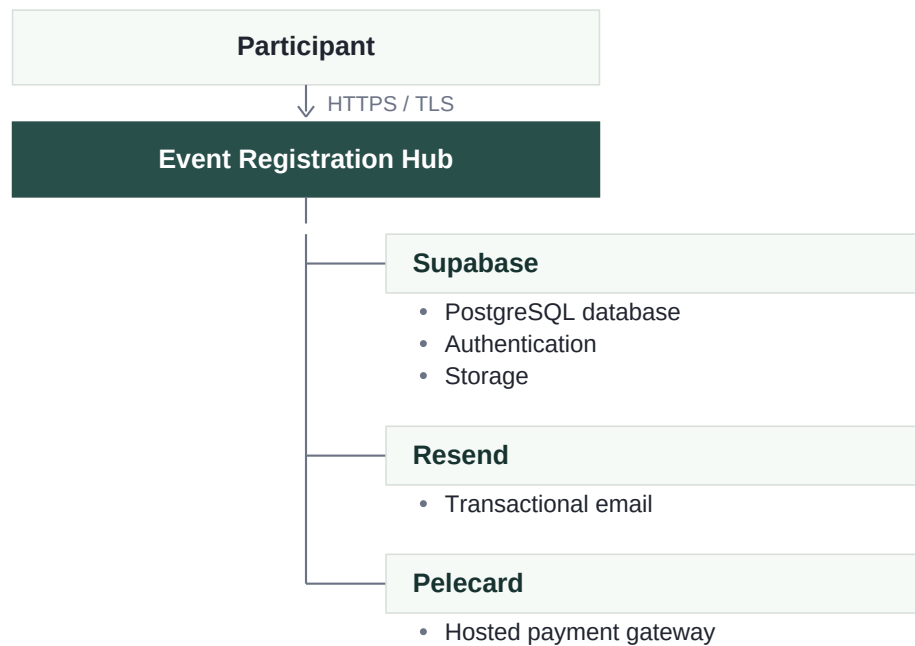
## Email Security

|                              |                                |
|------------------------------|--------------------------------|
| <b>Email provider</b>        | Resend                         |
| <b>Domain authentication</b> | SPF, DKIM, and DMARC supported |
| <b>Delivery logging</b>      | Enabled                        |

- Transactional emails (confirmations, payment requests, reminders) are sent from a verified sending domain.
- Confirmation and payment email delivery is logged for admin review.

## Infrastructure

The platform is built on established, managed infrastructure providers. Application traffic is served over a global edge network; database, authentication, storage, email, and payments run on dedicated managed services.



## Privacy

- Sensitive fields are not included in emails unless explicitly selected by the form owner.
- Managers only see the forms assigned to them; other events remain inaccessible.
- Receipt, debug, and payment gateway logs are restricted to administrators.
- Cancellation policy and privacy policy acceptance can be tracked per registration.
- Personal data is retained only as long as needed to operate the event registration service.

## Operational Security

- Login history recorded for admin review.
- Active sessions tracked with per-session revocation.
- Failed login tracking with automated account lockout.
- Payment logs, email delivery logs, and receipt sync logs are retained for audit.
- Dynamic inactivity logout based on the configured session timeout.

## Platform Availability

- Managed cloud infrastructure.
- Automated database backups.
- High-availability cloud services.
- Disaster recovery procedures.

## Data Residency

Customer data is stored within the configured Supabase project region. Application traffic is encrypted using HTTPS/TLS, and managed infrastructure provides encryption at rest for stored data.

## Security Principles

 **Least Privilege Access** **Role-Based Permissions** **Defense in Depth** **Secure Hosted Payments** **Row Level Security** **Continuous Security Improvements**

## Continuous Security Improvements

Security is treated as an ongoing program. Current focus areas include:

- Comprehensive Administrative Audit Log
- Application-Level Encryption for Sensitive Fields
- GDPR Self-Service Tools
- Administrator Security Dashboard

The platform is not currently ISO 27001, SOC 2, HIPAA, or PCI-DSS certified. Payment card processing is handled by the hosted payment provider, and the platform does not store raw card data.

## Support Contact

For security questions, procurement reviews, or to report a security concern, please contact [info@eventreghub.com](mailto:info@eventreghub.com).

## Document Information

|                       |                        |
|-----------------------|------------------------|
| <b>Document</b>       | Security Overview      |
| <b>Platform</b>       | Event Registration Hub |
| <b>Version</b>        | 2026.07                |
| <b>Generated</b>      | 11 September 2026      |
| <b>Classification</b> | Public                 |

This document is automatically generated from the current Event Registration Hub security configuration. The information reflects the platform configuration active on the date this document was generated.