SECURITY AND DATA

KEPT APART. KEPT SAFE.

How AVEO EOS keeps each company's records to itself, who can sign in and open what, how money moves, and how the API and webhooks are protected.

EVERY COMPANY APART

A SEALED SPACE FOR EACH COMPANY.

Every company runs in a sealed space of its own, on the same software AVEO runs its own events on.

A database for each company.

Each company has its own database with its own login. That login opens the company's own database and nothing else: not another company's, not EOS's platform records, not the ticket engine's.

Every request to EOS is tied to exactly one company before any code runs, and the data layer refuses to run without one, so a request can never reach the wrong company's records.

Its own ticket engine account.

Tickets, orders and check-ins are held in the company's own account on EOS's ticket engine, with a key of its own. The engine itself refuses one company's key on another's events.

Its own Stripe account.

Card payments are taken directly on the company's own Stripe account and paid out by Stripe to its bank. The booking fee buyers pay on top of their tickets, AVEO's only fee, is passed to AVEO by Stripe at the moment of payment. See Payments and Stripe.

Apart from AVEO's own events.

AVEO's own events and data run on separate database servers and networks. AVEO's staff set companies up, and manage their plans and fees, through a private, signed connection.

SIGNING IN.

- Staff sign in with their work email, which names their company. One email belongs to one company.
- Passwords of at least 12 characters; passwords found in known data breaches are refused.
- A human check on the sign-in form, and accounts that lock for a while after repeated wrong passwords.
- Two-step sign-in with an authenticator app or a passkey (Face ID, Touch ID, Windows Hello or a security key). Admins, managers and security managers must use one, and custom roles can be set to need it.
- Each company's sign-in keeps its own session, so a company's console and its sandbox stay apart even in one browser.
- Five wrong passwords for one account inside 15 minutes lock it for 15 minutes, wherever they come from, and its owner is emailed.
- A new browser signing in to an account emails its owner, and every password change is emailed and logged.
- Passwords are kept only as salted scrypt hashes, never as the password itself.

ACCESS

EXACTLY THE ACCESS EACH JOB NEEDS.

- There is no sign-up: an admin adds each person on the Team page, and they get an email to choose a password.
- Built-in roles for the office, the door and security, and custom roles where you tick the pages and features they open.
- Admins can set a temporary password that must be changed, sign someone out everywhere, reset their second factor or turn them off.
- Everyone at your company reads and signs AVEO EOS's policies before they use it.

EVERYTHING RECORDED.

- An audit trail records every change made by staff, with who made it and when.
- Every scan at the door is logged with who scanned, at which gate and on which device. A plan sets how many devices may scan at the same time; admins see each one and can free its place.
- A consent log keeps proof of consent, and every API key keeps a log of its requests for 30 days.

PAYMENTS.

- Buyers pay through Stripe's Payment Element: card details go to Stripe and never reach AVEO EOS.
- Each order is a direct charge on the company's own Stripe account, paid out by Stripe to its bank.
- Stripe's notices about payments arrive as signed webhooks; an order is marked paid only when Stripe confirms.

ON THE WEB.

- Every page is served over HTTPS.
- Console pages cannot be shown inside another website, and are kept out of search engines.
- Live shops are open to search engines; a sandbox's test shop never is.

CONNECTIONS

THE API AND WEBHOOKS.

KEYS	A secret key is shown once, when it is made, and kept only as a peppered hash, so neither the database nor its backups hold a usable key.
PERMISSIONS	Each key holds only the permissions it is given, and your plan sets the most it may have.
EXPIRY	Each key can expire after 7, 30, 90 or 180 days, a year, or never.
ADDRESSES	A key can be limited to IP addresses; a publishable key works only from the web addresses you allow.
BROWSERS	A secret key sent from a web page is refused. Publishable keys may only read events and start checkouts.
RATE LIMITS	Each key has a request limit a minute, and addresses that fail the key check again and again are made to wait.
WEBHOOKS	Sent only to https addresses on the public internet (private network addresses are refused), signed with each endpoint's own secret, which you can roll.

THE SANDBOX.

A sandbox never holds live Stripe keys, its test payments never count as money, its keys never work on your live company, and its shop is closed to search engines.

WHAT YOUR ADMINS CAN DO.

01 **Turn on two-step sign-in for everyone**
It is required for admins, managers and security managers; custom roles can be set to need it too.

02 **Give each person only what they need**
Use the built-in roles, or custom roles from Professional, and turn people off when they leave.

03 **Keep keys small and short-lived**
One key per use, only the permissions it needs, an expiry date, and the addresses it is used from.

04 **Check webhook signatures**
Trust a webhook only after its signature checks out against your endpoint's secret.

05 **Watch your scanning devices**
Plan and billing lists every phone and door app scanning your tickets; free the place of any you do not know.

AVEO

QUESTIONS ABOUT SECURITY?

Ask AVEO about how AVEO EOS protects your company's records, your team and your buyers, before or after you start.

ASK FOR A TRIAL	aveoevents.com/eos
DOCUMENTS AND GUIDES	documents@aveoevents.com
SUPPORT	support@aveoevents.com
API	aveoevents.com/eos/api

AVEO EOS is made and run by AVEO. 22 November 2026.