Data Security Overview

The hardened setup for consolidated reporting and AI
HospitalityOS Advisory | November 2026

Most hotel groups read the same numbers several times a day, in reports from the PMS, the POS, the spa system and a manual daily report. Putting them in one place only makes sense if that place is safer than the inboxes they land in now. This is our hardened setup, the one we recommend when owners or an IT provider will ask hard questions. It covers how we build it, what each control protects you from, and what we won't claim.

How we build it

The data lives in a dedicated Cloudflare account that you own and that holds nothing except this build. Your IT keeps the top administrator role. We work inside it with build roles only, and you can remove us in one step. The database, the code and the documentation stay with you either way.



Data moves one way. Nothing writes back to the PMS or POS.

What it runs on

Layer	Platform	How it is used	Independent attestations
Data layer and portal	Cloudflare Workers, D1, R2 and Access	Scheduled pulls, storage and the reporting portal. Data encrypted in transit (TLS) and at rest.	SOC 2 Type II, ISO 27001, ISO 27701, PCI DSS. Reports available to you as the account owner.
Property management	Your PMS, through its published API	Read-only. Scoped access such as OAuth 2.0 where the vendor supports it.	Your PMS vendor's own program. We collect its current reports during setup.
Restaurants, activities, spa	Your POS and other operating systems	Read-only reporting credentials or scheduled exports.	Each vendor's own program, collected the same way.
AI	Your ChatGPT Enterprise or Business workspace, or the OpenAI API	Answers questions over the reporting views only. It cannot reach the source systems.	SOC 2 Type 2. Business and API data is not used to train models by default.
Sign-in	Your Microsoft 365 or Google Workspace	Single sign-on and MFA through Cloudflare Access.	Your existing identity policies apply.

The hardened controls and what each one protects you from

Control	What we set up	What it protects you from
Dedicated account	One Cloudflare account that holds only this build, separate from your website and DNS.	A mistake or a compromised login here cannot reach your website, domains or email routing.
You hold the top role	Your IT keeps the Super Administrator role. We get build roles and nothing more.	We cannot add users, change billing or lock you out. Removing us takes one step.
Hardware keys for admins	Anyone with admin rights, on your side or ours, signs in with a physical security key.	A stolen password or a phishing link is useless without the key in hand.
Managed devices only	The portal opens only on laptops and phones your IT has enrolled.	Logins from personal, lost or unknown devices are refused, even with the right password.
Your sign-in, short sessions	Access runs through your company sign-in with MFA, by role, and sessions expire.	People who leave lose access the moment IT disables them. An unattended screen times out.
Read-only at the source	Every connection uses a dedicated read-only user or scoped key that you issue.	Nothing in the reporting layer can change a reservation, a rate or a check (until you authorize an ops layer).
Short-lived deploy tokens	Every token we deploy with is limited in permission and set to expire.	A leaked token is narrow in reach and soon dead.
Guest fields encrypted with your key	Any guest-level field is encrypted in the application with a key you hold.	Guest details stay unreadable to us by default and to anyone who copies the database.
Your eyes on the logs	Your IT gets the audit log role and an export of sign-ins, pulls and changes.	Every change we make is visible to someone who is not us.
No payment card data	Card numbers are never requested, pulled or stored.	The build stays outside your PCI scope. There is no card data here to lose.

For a team under 50 users these controls run on Cloudflare's free access tier. The added cost is a security key for each administrator and the time for your IT to enroll devices.

What we commit to in writing

1. **You own it.** The account, the database, the application code and the documentation are yours from day one.
2. **Guest data kept to a minimum.** Reporting runs on operating numbers such as occupancy, rate, revenue, covers and labor. Guest-level fields come in only if a report you ask for needs them, and you approve each one.
3. **Secrets stay in the vault.** API credentials sit in Cloudflare's encrypted secret store and never in code, email or chat.
4. **Fast notice.** If we confirm or reasonably suspect unauthorized access to anything we built or hold, your named contact hears from us within 24 hours of when we become aware, with what we know at that point. Updates follow as we learn more.
5. **Clean exit.** Remove our access at any time and everything keeps running. Any working copies we hold are deleted within 30 days of the engagement ending, confirmed in writing.

What we won't claim

HospitalityOS is an advisory firm. We do not hold our own SOC 2 report, and we won't describe a build as SOC 2 certified. The attestations on page one belong to the platforms. What we control is the design.

We set a United States location preference for the database. Cloudflare does not offer a US-only guarantee on this product outside its FedRAMP data centers, so we won't promise one.

Your IT team or provider is welcome to review the configuration before anything connects to live data, and we'd rather they did.

What we need from you to start

1. A new Cloudflare account registered to your company, with your IT as Super Administrator and us invited as a member. The paid developer plan starts at about $5 a month.
2. A read-only user or API key for each source system, issued by your team.
3. The sign-in groups that decide who sees which reports, and the list of devices to enroll.
4. Your IT and security policies, protocols and vendor requirements, including any security questionnaire you use. We review them before the build starts and confirm in writing that we will conform. If there is anything we can't meet, we tell you then, before any work begins.
5. One named security contact, on your team or at your IT provider.

HospitalityOS is led by Peter Mack, who founded Collective Retreats (10 locations, acquired 2025) and was VP Sales Strategy and Operations at Starwood (800+ hotels). peter@hospitalityos.tech
Platform attestations are as published by each vendor as of November 2026 and are theirs to maintain. Current reports are available from each vendor on request.