Data Security Overview: Enterprise Setup

The Fortune 500-level configuration on AWS and Amazon Bedrock
HospitalityOS Advisory | November 2026

This is the strongest setup we build. Your data, the reporting portal and the AI all sit inside one AWS account that you own, on a private network, in United States data centers, encrypted with keys you control. It is built from the same AWS services and design patterns that banks, hospital systems and large public companies run on. It costs more to run than our standard setup. This document covers what you get for that, what each control protects you from, and what we won't claim.

How we build it

Everything lives in a dedicated AWS account registered to your company. Your IT holds the root login and the administrator role. We work through a build role that you grant, that requires MFA, and that you can switch off in one step. The database and the AI sit on a private network with no public address. The AI is Amazon Bedrock, reached over a private connection, so a question about your numbers never crosses the public internet and never reaches the company that made the model.



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

What it runs on

Layer	Service	What it does
Private network	Amazon VPC with private subnets and AWS PrivateLink	The database and the AI have no public internet address.
Database and storage	Amazon Aurora (PostgreSQL) and Amazon S3	Holds the reporting data. Encrypted at rest with your key, backed up automatically, public access blocked.
AI	Amazon Bedrock	Answers questions over the reporting views only. Prompts and answers are not shared with model makers or used for training. US Regions only.
Keys and secrets	AWS KMS and AWS Secrets Manager	You own the encryption key. Source-system credentials are stored encrypted, never in code, email or chat.
Portal and sign-in	Amazon CloudFront, AWS WAF and your Microsoft 365 or Google sign-in	Single sign-on with MFA, by role, behind a web application firewall.
Monitoring	AWS CloudTrail, Amazon GuardDuty, AWS Security Hub and AWS Config	Every administrative action is recorded. Threat detection runs around the clock.

The certifications each platform holds, and the standards this build is configured to meet, are listed under Compliance.

The controls and what each one protects you from

Control	What we set up	What it protects you from
Your own AWS account	One account that holds only this build. Your IT keeps the root login and the administrator role.	We cannot lock you out, change billing or add users. Nothing is shared with any other client. Removing us takes one step.
Private network	The database and the AI sit in private subnets. Bedrock is reached through AWS PrivateLink.	There is no database address on the internet to attack, and AI traffic never travels over the public internet.
AI that stays inside	Amazon Bedrock runs the model inside AWS. Prompts and answers are not shared with the model maker and are not used for training.	Your numbers and any guest details do not end up in someone else's model.
Encryption keys you control	The database, storage, backups and logs are encrypted with a key held in your AWS KMS.	Disable the key and the data is unreadable, to us and to anyone holding a copy.
United States only	The build is pinned to US Regions, AI processing uses a US-only profile, and an account policy blocks every other Region.	A clear answer for an owner, lender or insurer who asks where the data lives.
Least-privilege access with MFA	People sign in through your company identity. Admins use hardware security keys. Our build role is scoped and time-limited.	A stolen password is useless on its own. People who leave lose access the moment IT disables them.
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).
Logged and watched	CloudTrail records every action to a locked bucket your IT controls. GuardDuty and Security Hub raise alerts on unusual behavior.	Every change we make is visible to someone who is not us, and odd activity is flagged without anyone having to go looking.
Web firewall and managed devices	AWS WAF sits in front of the portal. Your sign-in policy limits access to devices IT has enrolled.	Common web attacks are blocked at the edge. Logins from unknown devices are refused.
Backups you can restore	Encrypted daily backups with point-in-time recovery, and a restore test before go-live.	A bad change, a deletion or a ransomware event is recoverable.
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.

Compliance: what the platforms are certified for

These certifications belong to the platforms. Independent auditors test them every year, and as the AWS account owner you can download the current AWS reports yourself from AWS Artifact.

Platform	Independent certifications and reports
AWS infrastructure (every service in this build)	SOC 1, SOC 2 and SOC 3 (Type 2 reports). ISO 27001, 27017, 27018, 27701, 22301 and 9001. PCI DSS Level 1 service provider. CSA STAR Level 2. FedRAMP.
Amazon Bedrock (the AI)	In scope for the AWS SOC 1, 2 and 3 reports and the ISO certifications above. HIPAA eligible. CSA STAR Level 2. ISO 42001, the standard for managing AI systems.
Sign-in (Microsoft 365 or Google Workspace)	Each publishes its own SOC 2 Type II report and ISO 27001 certification. Your existing identity policies apply.
Your PMS, POS and other source systems	Each vendor's own program. We collect their current reports during setup and tell you if any are missing.

Compliance: what this build is configured to meet

A build like this is not certified on its own. Certification is something an organization earns through an audit over time. What we can do, and show you, is configure the build to recognized standards and leave the evidence in your account.

Standard	How this build meets it	Where that leaves you
CIS AWS Foundations Benchmark	AWS Security Hub checks the account against it continuously.	Findings fixed before go-live. Your IT sees the score at any time.
AWS Foundational Security Best Practices	Checked continuously by AWS Security Hub, alongside the CIS benchmark.	Same. Findings fixed before go-live.
AWS Well-Architected Framework, security pillar	The design follows it: identity, detection, network protection, data protection, incident response.	Design review documented and handed to you.
SOC 2 security criteria	The controls line up with what a SOC 2 auditor tests: access, encryption, logging, change control, backup.	Supports your own audit or a lender's review. Not a certification.
PCI DSS	No card data is requested, pulled or stored.	Out of scope by design.
State privacy laws such as CCPA	Guest data is kept to a minimum and can be found and deleted on request.	Supports your obligations. Your counsel decides what applies.

How it compares with our standard setup

Both are sound. The standard setup is right for most groups. This one is for owners, lenders or IT providers who want the tighter answer on every line.

	Standard setup (Cloudflare and ChatGPT)	Enterprise setup (AWS and Bedrock)
You own the account, code and data	Yes	Yes
AI provider does not train on your data	Yes	Yes
Database and AI on a private network	No. Encrypted traffic over the internet	Yes
Encryption keys you hold and can revoke	Guest fields only	Everything
United States-only data guarantee	No	Yes
Threat detection and configuration monitoring	Audit logs	Continuous, with alerts
Running cost, paid to the platform	About $5 a month	A few hundred dollars a month (our estimate)

AWS bills you directly. We give you a written cost estimate before the build starts.

What we commit to in writing

1. **You own it.** The AWS 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 AWS Secrets Manager 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 in this document belong to AWS. What we control is the design.

"Fortune 500-level" describes the platform and the controls: the same AWS services and patterns large enterprises use. It is not a certification, and no setup is breach-proof. AWS secures the platform. The configuration is our job, and yours to review.

The AI model is chosen at build time from those Bedrock offers with US-only processing. If a model you want is only available with global routing, we tell you and don't use it without your say.

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 AWS account registered to your company, with your IT holding the root login and the administrator role, and a build role granted to us.
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
AWS attestations and Amazon Bedrock data handling are as published by AWS as of November 2026 and are theirs to maintain.