DeployReady Trust Center

Effective Date: April 22, 2026
Version: v1.0.0
Last Updated: April 22, 2026
Published at: capstonehorizon.com/trust
Contact: security@capstonehorizon.com

What DeployReady Is

DeployReady is a SaaS platform built by Capstone Horizon LLC that helps small businesses and government contractors analyze federal solicitations and generate compliant proposal drafts. Customers upload publicly available solicitations (from SAM.gov or similar sources), maintain a company profile, and receive AI-assisted proposal outputs grounded in their actual capabilities.

Our security philosophy: FCI-adjacent by design. DeployReady is not a federal information system and is not designed to process Federal Contract Information (FCI), Controlled Unclassified Information (CUI), or any other restricted government data. We built the product this way on purpose. Our Terms of Service prohibit uploading restricted data, and our product posture -- from data architecture to LLM routing -- reinforces that boundary. We voluntarily implement the 15 baseline security controls from FAR 52.204-21 because they represent a sound commercial baseline for protecting our customers' business data, not because we are required to.

Architecture at a Glance

Hosting: DeployReady runs on Railway, which hosts the application on AWS infrastructure in the us-east-1 region (Northern Virginia). All customer data remains in the United States.

Database: Railway Postgres with AES-256 encryption at rest (Railway default). Daily automated snapshots with 7-day retention. All database traffic is encrypted in transit.

Tenant Isolation: Every data read and write in the application binds to the requesting tenant's ID derived from the server-side session (`req.tenantId`). This app-layer enforcement runs on every query. Additionally, Postgres Row-Level Security (RLS) policies under the `tenant_isolation` policy are applied at database startup on 19 tenant-scoped tables, including solicitations, proposals, company profiles, file vault, credentials, and audit logs. This gives us defense-in-depth: even a misconfigured query cannot return another tenant's records if the database role permits RLS enforcement.

Authentication: Users authenticate with email and password. Passwords are hashed using scrypt (N=16384, 64-byte derived key, random per-user salt) and compared using constant-time comparison (`timingSafeEqual`). Brute-force protection limits login attempts to 5 per IP+email combination per 15-minute window. Sessions are server-side and persisted to the database, with an in-memory L1 cache per request. Multi-factor authentication for administrative accounts is on the roadmap for Q3 2026.

TLS: All ingress to `app.capstonehorizon.com` routes through Railway's HTTPS termination (TLS 1.2 minimum). The application itself rejects any non-HTTPS request in production (308 redirect for safe methods, 403 for unsafe methods) and sends `Strict-Transport-Security: max-age=31536000;`

`includeSubDomains` on every response. There is no unencrypted HTTP path to the application.

Data You Control

As a DeployReady customer, you own everything you bring in and everything the product generates for you. This includes:

- Your company profile (capabilities, past performance, personnel, certifications)
- Solicitations you upload or import
- Generated proposal drafts
- Files stored in the vault

Capstone Horizon does not claim ownership of your content. You can request deletion of your data at any time, and we will process it within 30 days. See our Data Handling Policy for retention schedules and deletion procedures.

Scope Boundaries: What We Do Not Process

DeployReady is not designed or authorized to hold the following data categories:

- Federal Contract Information (FCI) as defined at FAR 4.1901
- Controlled Unclassified Information (CUI) as defined at 32 CFR 2002.4
- Classified National Security Information at any classification level
- ITAR-controlled technical data or EAR-controlled export-controlled data
- Protected Health Information (PHI) under HIPAA
- Any information you are contractually obligated to protect under DFARS 252.204-7012 or equivalent

These are defined as Prohibited Data in our Terms of Service, Section 4. Uploading Prohibited Data violates our Terms and may result in immediate suspension of your account. DeployReady is appropriate for analyzing publicly available solicitations (such as those from SAM.gov) and generating proposal drafts from your company's own, non-restricted capability data.

FAR 52.204-21 compliance boundary note: The covered-contractor-information-system boundary under FAR 52.204-21 lives within your organization's own systems, not within DeployReady. Using DeployReady does not make it a covered contractor information system; it is a commercial SaaS tool for publicly available solicitation work.

AI Safety and Anti-Fabrication

Government proposals carry legal risk. A proposal that invents personnel, past performance, or certifications can expose a contractor to False Claims Act liability. DeployReady's proposal engine is built around a firm "no fabrication" rule set (v2 rules, shipped April 21, 2026, commit 54e0bde).

In plain English, the rules are:

1. Only your profile is authoritative. The proposal engine may only use facts from your company profile block. It cannot infer, embellish, or extrapolate.

2. No invented personnel. The engine cannot create names, roles, or qualifications for people who are not in your profile.
3. No invented past performance. The engine cannot fabricate contract numbers, dollar values, client names, or performance narratives.
4. No invented clearances. The engine cannot claim security clearances for personnel or the organization that are not in the profile.
5. No invented language fluency. The engine cannot claim foreign language capability that is not explicitly listed.
6. No invented quantitative claims. The engine cannot generate performance metrics, staffing numbers, or cost figures that are not in the profile.
7. Restricted compliance matrix vocabulary. Compliance matrix entries are limited to three labels: "ADDRESSED VIA RECRUITMENT," "PARTIALLY COMPLIANT," and "WILL BE COMPLIANT AT PHASE-IN." "ADDRESSED VIA TEAMING" is only permitted if a named teaming partner appears in the profile.
8. No narrative from skill tags. The engine cannot construct a past performance narrative from a list of skills alone.
9. Default gap framing is "will recruit." When a capability gap is detected, the default framing is that the company will recruit for it -- not that it already has the capability.

The capability-gap detection system surfaces personnel, clearance, and language gaps to you before generation, so you can decide how to handle them rather than discovering them after the fact.

For the full technical writeup, see AI Safety and Anti-Fabrication.

Subprocessors

DeployReady uses a small set of third-party vendors to deliver the service. We only engage subprocessors in the United States. The full list is at capstonehorizon.com/legal/subprocessors. Summary:

Subprocessor	Role
Railway	Application hosting and database (AWS us-east-1)
Stripe	Payment processing
OpenAI	LLM inference for proposal generation
Anthropic	LLM inference for proposal generation
xAI (Grok)	LLM inference for proposal generation
Resend	Transactional email (login, notifications, receipts)

We will give 30 days' advance notice before adding any new subprocessor that touches customer data.

Security Practices: The FAR 52.204-21 Baseline

We voluntarily implement the 15 basic safeguarding controls from FAR 52.204-21. Below is a plain-English summary organized into four areas. The detailed mapping with status and evidence pointers is in our internal

self-attestation document, available to enterprise customers and APEX advisors on request.

Access Control. Access to the system requires authentication on every route. Every API endpoint that touches data is gated by a valid server-side session. Within the platform, users are assigned roles (owner, admin, member), and role-based permissions limit which functions each role can perform. Session tokens are persisted to the database and bound to a tenant on each request. External connections use TLS 1.2 or higher for all ingress.

Identity and Authentication. All users are identified and authenticated before gaining access. Password hashing uses scrypt with a per-user random salt. Failed login attempts are rate-limited. Account and session management is handled server-side. MFA for administrative accounts is on the Q3 2026 roadmap.

Physical Security. DeployReady has no physical infrastructure. Physical access controls, visitor management, and media disposal for the underlying hardware are governed by Railway and AWS. AWS us-east-1 maintains SOC 2 and ISO 27001 certifications.

System and Communications Protection. All external traffic is protected by TLS, with application-layer HTTPS enforcement and HSTS headers set on every response. Railway's network architecture provides segmentation between application tiers. The application uses Drizzle ORM, which prevents raw SQL injection by design. TypeScript strict-mode compilation reduces a category of runtime type errors. Dependencies are audited on every push and pull request via a GitHub Actions workflow that blocks new high or critical vulnerabilities. Two dependencies (`xlsx` and `drizzle-orm`) carry known high-severity advisories that are grandfathered on a documented allow-list with compensating controls and a scheduled migration path. The audit log captures authentication events (login success, login failure, logout), profile creation and updates, solicitation uploads, proposal generation and deletion, user invitations, and data exports, with user ID, tenant ID, email, role, IP address, user agent, resource identifier, and timestamp on every entry.

Roadmap

We build in public about our security posture. Here is what is coming and when:

Item	Target	Notes
MFA for administrative accounts	Q3 2026	TOTP-based, enforced for owner and admin roles
xlsx library migration (replace SheetJS)	Q3 2026	Closes known prototype pollution + ReDoS advisory
Drizzle ORM major version bump	Q2 2026	Closes known advisory; schema migration tested in staging first
File upload malware scanning	Q4 2026	ClamAV or equivalent on file vault uploads
SOC 2 Type I readiness	Q4 2026	Contingent on customer demand; gap assessment begins Q3
External penetration test	6-12 months post-launch	Third-party, scoped to application and API

Item	Target	Notes
Incident response tabletop exercise	Q1 2027	Initial tabletop with written post-mortem
FedRAMP (Path A)	When a federal agency becomes a direct customer	Not applicable to current commercial posture

Contact

- Security questions, vulnerability reports: security@capstonehorizon.com
- Privacy requests, data deletion: privacy@capstonehorizon.com
- Legal: Capstone Horizon LLC, 7782 Rose Rock Way, Las Vegas, NV 89113
- Website: capstonehorizon.com