FAR 52.204-21 Basic Safeguarding Controls -- Self-Attestation

Document type: Internal -- available to enterprise customers and APEX advisors on request
Attestation Date: April 22, 2026
Version: v1.1.0
Last Updated: April 22, 2026
Signer: David Diaz, Founder/CEO, Capstone Horizon LLC
Next scheduled attestation: January 2027
Supersedes: v1.0.0 (April 22, 2026)

1. Purpose

This document records Capstone Horizon LLC's voluntary self-attestation against the 15 basic safeguarding controls in FAR 52.204-21 (Federal Acquisition Regulation Subpart 4.19, "Basic Safeguarding of Covered Contractor Information Systems"), as published in the November 2021 revision of the clause.

Capstone maintains this attestation as an internal security baseline document. It is not prepared in response to a contract clause, a prime contractor's flow-down, or a government audit demand. It is prepared because these 15 controls represent a sound commercial security baseline appropriate for a SaaS platform that serves government contractors.

2. Scope Statement: We Are NOT a Covered Contractor Information System

DeployReady is not a covered contractor information system under FAR 52.204-21.

FAR 52.204-21 applies to a contractor's information system that "processes, stores, or transmits Federal contract information." Federal contract information (FCI) is defined at FAR 4.1901 as "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government."

DeployReady is designed and operated as a pre-award solicitation-analysis and proposal-generation tool. It is used with publicly available solicitations (primarily from SAM.gov). Our Terms of Service Section 4 explicitly prohibits upload of FCI, CUI, Classified National Security Information, and any other restricted government data. The covered-contractor-information-system boundary lives within each customer's own environment, not within DeployReady.

We implement these 15 controls because they are a sound commercial security baseline, not because we are legally required to under FAR 52.204-21. This distinction matters and is stated clearly here so that customers, APEX advisors, and potential primes understand the posture.

3. Mapping Table

The 15 controls are at FAR 52.204-21(b)(1)(i) through (xv). Paragraph numbering below matches the current (Nov 2021) FAR revision exactly. Status definitions:

- DONE -- Control is fully implemented in production.
- PARTIAL -- Control is partially implemented; gap and roadmap noted.
- N/A (INHERITED) -- Control is not applicable to a cloud-hosted SaaS with no physical infrastructure; implementation is inherited from Railway / AWS.

b.1.i -- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices.

Field	Detail
Status	DONE
Our implementation	Every data-bearing API route in `app.capstonehorizon.com` requires a valid server-side session. Unauthenticated requests are rejected. The session includes a `tenantId` derived at login and bound to `req.tenantId` on every request. All database queries include an explicit tenant filter. There is no unauthenticated data access path.
Evidence pointer	Session middleware in `server/auth.ts`; route guards on all `/api/*` endpoints; audit log records every login event (`auth.login`) and failed login (`auth.login_failed`).
Gap	None.
Roadmap	N/A

b.1.ii -- Limit information system access to the types of transactions and functions authorized users are permitted to execute.

Field	Detail
Status	DONE
Our implementation	Users are assigned one of three roles within a tenant: owner, admin, or member. Role is stored in the `users` table and checked at the route level for privileged operations (user management, data export, billing, account deletion). Members cannot perform administrative functions.
Evidence pointer	Role field in `users` table; role-check middleware in route handlers for admin-only endpoints.

Audit coverage (as of v1.1)	`auth.login`, `auth.login_failed`, `auth.logout`, `user.invite`, `profile.create`, `profile.update`, `solicitation.upload`, `solicitation.analyze`, `proposal.generate`, `proposal.delete`, `proposal.export`, `data.export`. Every entry records user ID, email, tenant ID, role, IP address, user agent, resource type and ID, and timestamp.
Gap	No MFA audit events yet (MFA itself is on Q3 2026 roadmap). No UI for end-user audit log review (logs are queryable by owner via database access).
Roadmap	MFA events + in-app audit log viewer: Q3 2026

b.1.iii -- Verify and control/limit connections to and use of external information systems.

Field	Detail
Status	PARTIAL
Our implementation	All inbound connections to `app.capstonehorizon.com` are routed through Railway's HTTPS termination (TLS 1.2 minimum). All outbound connections from the application to subprocessors (OpenAI, Anthropic, xAI, Stripe, Resend) use TLS. HTTP-to-HTTPS redirect is enforced at the Railway ingress layer.
Application-layer enforcement	The Express app (`server/index.ts`) sets `app.set("trust proxy", 1)` and rejects non-HTTPS traffic in production: 308 redirect for GET/HEAD, 403 JSON rejection for unsafe methods. `Strict-Transport-Security: max-age=31536000; includeSubDomains` is set on every response alongside `X-Frame-Options: DENY`, `X-Content-Type-Options: nosniff`, `Referrer-Policy: strict-origin-when-cross-origin`, and a restrictive `Permissions-Policy`.
Gap	HSTS preload registration not yet requested. Outbound connections are controlled at the application layer only (no network-layer egress allow-list).
Roadmap	HSTS preload registration: Q3 2026. Network-layer egress allow-list: evaluate alongside GovCloud migration (Q1 2027).

b.1.iv -- Control information posted or processed on publicly accessible information systems.

Field	Detail
Status	PARTIAL

Our implementation	The marketing site at `capstonehorizon.com` is managed by Capstone (Squarespace). The marketing site at `deployready.capstonehorizon.com` is a separately-deployed static bundle with no database access. The Trust Center at `deployready.capstonehorizon.com/trust` and its linked compliance documents are published by Capstone. Customer-uploaded content is never exposed publicly; it is scoped to authenticated tenant sessions only. There is no anonymous upload path.
Evidence pointer	Static marketing files in `client/public/marketing/`; separate route handler in `server/static.ts`; authentication middleware on all `/api/*` endpoints.
Gap	Content review process for public pages is informal; a documented content-review checklist is a roadmap item. No automated scanner verifies that the public marketing site does not contain FCI.
Roadmap	Document public-content review checklist: Q3 2026. Automated lint rule to flag prohibited keywords in marketing pushes: Q3 2026.

b.1.v -- Identify information system users, processes acting on behalf of users, or devices.

Field	Detail
Status	DONE
Our implementation	Every authenticated session is tied to a specific userId, tenantId, email, and role. Every audit log entry records these identifiers plus IP address and user agent. All system processes that touch customer data act under an identified tenant context.
Evidence pointer	`audit_logs` table schema; session object construction in `server/auth.ts`.
Gap	None.
Roadmap	N/A

b.1.vi -- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Field	Detail
Status	DONE
Our implementation	Authentication requires email and password. Passwords are hashed using scrypt (parameters: N=16384, 64-byte derived key, random salt per user). Hashes are stored in the `users` table as `salt:hash`. Comparison uses Node.js `timingSafeEqual` to prevent timing-based enumeration. Failed logins are rate-limited to 5 attempts per IP+email combination per 15-minute window.

Evidence pointer	`server/auth.ts`; scrypt configuration in password utility; rate-limit middleware.
Gap	MFA (multi-factor authentication) for admin and owner accounts is not yet implemented. It is on the roadmap.
Roadmap	MFA for admin/owner accounts (TOTP): Q3 2026

b.1.vii -- Sanitize or destroy information system media containing Federal contract information before disposal or release for reuse.

Field	Detail
Status	N/A (INHERITED)
Our implementation	DeployReady does not own or manage physical storage media. All storage is on Railway-managed infrastructure (AWS us-east-1 EBS and RDS volumes). Media sanitization and disposal are governed by Railway's and AWS's policies, which include secure media destruction consistent with NIST 800-88 guidelines.
Evidence pointer	AWS media decommissioning policy; Railway security documentation.
Gap	Capstone has no direct visibility into specific media disposal events; we rely on inherited controls.
Roadmap	N/A; dependency on Railway/AWS.

b.1.viii -- Limit physical access to organizational information systems, equipment, and respective operating environments to authorized individuals.

Field	Detail
Status	N/A (INHERITED)
Our implementation	DeployReady has no physical data center presence. All infrastructure runs on Railway / AWS us-east-1. Physical access controls for AWS facilities are governed by AWS, which maintains SOC 2 Type II and ISO 27001 certifications, including rigorous physical access management.
Evidence pointer	AWS Compliance documentation; Railway's infrastructure security page.
Gap	None -- Capstone has no physical infrastructure to protect.
Roadmap	N/A

b.1.ix -- Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

Field	Detail
Status	N/A (INHERITED)
Our implementation	Capstone has no physical facility where visitor management, physical-access logging, or physical-access-device management is applicable. All three sub-requirements of the current FAR (ix) -- visitor escort, physical access audit logs, and physical access devices (badges, keys, biometrics) -- are inherited from Railway / AWS. AWS maintains physical access logs and device management as part of its SOC 2 Type II and ISO 27001 programs. Capstone operates as a fully remote company with no physical infrastructure, and maintains full logical audit logs (the `audit_logs` table) covering all authenticated user actions in the application.
Evidence pointer	AWS physical security controls; AWS physical access log retention practices; Capstone `audit_logs` table covers all logical access.
Gap	N/A for physical controls. Logical audit log coverage for MFA events pending MFA roll-out (Q3 2026).
Roadmap	MFA audit events: Q3 2026

b.1.x -- Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems.

Field	Detail
Status	DONE
Our implementation	All external traffic enters through Railway's TLS-terminated HTTPS ingress. Railway provides network segmentation between the application tier and the database tier. Database access from the application uses TLS-encrypted connections. There is no direct public database access path. Outbound API calls to subprocessors use TLS.
Evidence pointer	Railway network architecture; Railway Postgres connection string uses SSL; application database connection config in `server/db.ts`.
Gap	None at current scale.
Roadmap	N/A

b.1.xi -- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Field	Detail
Status	DONE (INHERITED)

Our implementation	Railway implements network segmentation for its hosted applications on AWS. The DeployReady application is not deployed in the same subnet as the Postgres database; Railway manages the separation. The database is not publicly accessible; it is accessible only from the application within Railway's internal network. The marketing site, application, and database each run in logically separated contexts.
Evidence pointer	Railway network architecture documentation; Railway Postgres access controls; separate Railway services for app and DB.
Gap	Capstone does not manage these subnets directly and relies on Railway's architecture.
Roadmap	N/A

b.1.xii -- Identify, report, and correct information and information system flaws in a timely manner.

Field	Detail
Status	PARTIAL
Our implementation	Dependency vulnerabilities are identified using `npm audit` integrated into the CI pipeline (`.github/workflows/ci.yml`). The workflow runs on every push and pull request, plus a weekly scheduled run, and blocks new high or critical vulnerabilities. A documented allow-list (`scripts/ci-audit-check.sh`) grandfathers two known-unfixable-today packages (`xlsx` and `drizzle-orm`), each with compensating controls and a migration target. Application errors are captured in Railway logs and reviewed by the engineering team. Security-relevant bug reports are routed to security@capstonehorizon.com with a 2-business-day acknowledgment SLA and 10-business-day remediation plan SLA.
Gap	No automated SAST (static analysis) in the pipeline. Allow-listed vulnerabilities (`xlsx`, `drizzle-orm`) carry residual risk until migration completes (Q2-Q3 2026).
Roadmap	Add SAST scanning (CodeQL or equivalent): Q4 2026. Close allow-listed vulnerabilities: Q2 2026 (drizzle), Q3 2026 (xlsx).

b.1.xiii -- Provide protection from malicious code at appropriate locations within organizational information systems.

Field	Detail
Status	PARTIAL

Our implementation	At the application layer: all database interactions use Drizzle ORM, which prevents raw SQL injection by construction; TypeScript strict-mode is enforced, reducing a class of runtime type confusion errors; all API handlers validate inputs with Zod schemas. At the infrastructure layer: Railway provides network-level protection against common attack vectors. HTTPS is enforced at both the Railway load balancer and the Express app layer, with HSTS headers set on every response. Customer-uploaded files are stored but not executed on the server.
Evidence pointer	Drizzle ORM usage throughout `server/*.ts`; Zod validation in route handlers; HTTPS + HSTS enforcement in `server/index.ts`.
Gap	No Web Application Firewall (WAF). No anti-malware scanning of uploaded files in the file vault. No content disarm and reconstruction (CDR) for uploaded documents.
Roadmap	File upload malware scanning: Q4 2026. WAF: evaluate alongside SOC 2 gap assessment Q3 2026.

b.1.xiv -- Update malicious code protection mechanisms when new releases are available.

Field	Detail
Status	PARTIAL
Our implementation	Application-layer dependency definitions (`package.json`) are refreshed via weekly automated `npm audit` runs plus on-demand updates when security advisories are issued. When a dependency used for security-relevant behavior (such as the scrypt implementation, session store, or ORM) publishes a new release, it is evaluated within the 10-business-day remediation SLA. Infrastructure-layer malicious code protections (AWS GuardDuty, managed-host protections on the Railway/AWS substrate) are updated automatically by the provider.
Evidence pointer	CI pipeline weekly schedule in `.github/workflows/ci.yml`; Incident Response Plan SLAs; Railway and AWS managed-update practices.
Gap	No CI-integrated automated PR-creation for dependency updates (Dependabot or Renovate). Updates are currently review-triggered rather than push-triggered.
Roadmap	Enable Dependabot for security updates on the deploy-ready repository: Q2 2026. Evaluate Renovate for broader dependency management: Q3 2026.

b.1.xv -- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Field	Detail

Status	PARTIAL
Our implementation	Periodic scanning of the codebase and its dependencies is performed weekly by the CI pipeline (`npm audit` on schedule). On-demand scans run on every push and pull request. Infrastructure-level scanning of the Railway/AWS substrate is performed continuously by the provider. Real-time scanning of files as they are uploaded, downloaded, opened, or executed is not currently implemented for customer-uploaded files in the file vault; uploads are stored as-is and served back only to the authenticated owner.
Evidence pointer	CI pipeline schedule in `.github/workflows/ci.yml` (cron 'weekly'); AWS GuardDuty and managed-host protections; Incident Response Plan.
Gap	No real-time anti-malware scanning of file uploads to the vault. No deep content inspection on upload. The application mitigates by never executing uploaded content server-side and serving only to the authenticated owner, but this does not satisfy the full FAR (xv) real-time requirement.
Roadmap	File upload malware scanning (ClamAV via Lambda or equivalent): Q4 2026. This is the primary remaining gap against current FAR 52.204-21.

4. Summary

Control	Status
b.1.i -- Limit access to authorized users	DONE
b.1.ii -- Limit access to authorized transactions/functions	DONE
b.1.iii -- Verify and control external connections	PARTIAL
b.1.iv -- Control info on public systems	PARTIAL
b.1.v -- Identify users, processes, devices	DONE
b.1.vi -- Authenticate users before access	DONE
b.1.vii -- Sanitize/destroy media before disposal	N/A (INHERITED)
b.1.viii -- Limit physical access	N/A (INHERITED)
b.1.ix -- Escort visitors + physical access logs + devices	N/A (INHERITED)
b.1.x -- Monitor/protect communications at boundaries	DONE
b.1.xi -- Subnetworks for public components	DONE (INHERITED)
b.1.xii -- Identify/report/correct system flaws	PARTIAL
b.1.xiii -- Provide protection from malicious code	PARTIAL

b.1.xiv -- Update malicious code protection mechanisms	PARTIAL
b.1.xv -- Periodic + real-time scans	PARTIAL

Summary: 6 DONE (incl. DONE INHERITED), 6 PARTIAL, 3 N/A (INHERITED)

All partial controls have documented remediation plans with Q2 2026 -- Q1 2027 target dates.

5. Version History

Version	Date	Change
v1.0.0	April 22, 2026	Initial attestation. Audit logging wired for 12 event types, app-layer HTTPS redirect + HSTS in force, CI-integrated `npm audit` gate with documented allow-list, cross-tenant isolation probe script available. Paragraph numbering followed a legacy NIST 800-171 Rev 1 era mapping that predated the current Nov 2021 FAR 52.204-21 clause.
v1.1.0	April 22, 2026	Renumbered to align with FAR 52.204-21 (Nov 2021). Consolidated legacy (ix)/(x)/(xi) physical-access items into current single (ix). Added explicit assessments for current (xiv) Update malicious code protection mechanisms when new releases are available, and current (xv) Perform periodic scans + real-time scans of files from external sources -- both previously covered only in part under the older combined malicious-code entry. Re-tallied summary counts (6 DONE / 6 PARTIAL / 3 N/A, total 15). Content of each retained control unchanged from v1.0.0; only paragraph numbering and the two new entries were added.

6. Attestation and Signature

I, David Diaz, as Founder and CEO of Capstone Horizon LLC, attest that the information in this document accurately reflects the current security posture of the DeployReady platform as of the Attestation Date stated above, to the best of my knowledge. This attestation is provided voluntarily and does not constitute a certification under any federal contract clause.

Signer: David Diaz
Title: Founder / CEO, Capstone Horizon LLC
Attestation Date: April 22, 2026

Signature: _____

Contact

Capstone Horizon LLC
5110 W Jeffrey Rd, Tucson, AZ 85757

security@capstonehorizon.com
capstonehorizon.com