DeployReady Data Handling Policy

Effective Date: April 22, 2026
Version: v1.0.0
Last Updated: April 22, 2026
Published at: capstonehorizon.com/legal/data-handling-policy
Contact: security@capstonehorizon.com | privacy@capstonehorizon.com

1. Purpose and Scope

This policy describes how Capstone Horizon LLC ("Capstone," "we," "us") collects, stores, processes, transmits, retains, and deletes data within the DeployReady SaaS platform. It applies to all data submitted to or generated by DeployReady by customers and their end users ("Tenant Data"), as well as operational data generated by the platform itself.

This policy is intended for internal operations teams, enterprise customers evaluating DeployReady for procurement, and APEX or compliance advisors reviewing our data practices.

2. Data Categories

The following categories of data are processed within DeployReady:

Category	Description	Source
Account credentials	Email address, scrypt-hashed password, role assignment	Customer on registration
Company profile	Business name, NAICS codes, capabilities, certifications, past performance, personnel (names and roles), teaming partners	Customer input
Solicitation data	Solicitation documents, requirement text, PWS/SOW uploads	Customer upload (must be publicly available per ToS Section 4)
Generated proposals	AI-assisted proposal drafts produced by the platform	System generated from customer profile + solicitation
File vault contents	PDFs and documents stored by the tenant	Customer upload
Audit logs	Action records including userEmail, userId, tenantId, action type, resource, IP address, user agent, timestamp, success flag	System generated

Category	Description	Source
Billing data	Payment method, billing address, transaction history (processed by Stripe; Capstone retains Stripe customer ID and plan metadata only)	Customer during checkout
Usage data	Session records, API call metadata, error logs	System generated
Transactional email metadata	Login notifications, system alerts, receipt confirmations (processed by Resend)	System generated

3. Data Classification

All Tenant Data processed within DeployReady is classified as Tenant Confidential. This means:

- Data is accessible only to authenticated users within the same tenant organization.
- Capstone personnel access Tenant Data only when required to provide support or investigate a security incident, under a logged and authorized session.
- Tenant Confidential data is not shared with any third party except the named subprocessors in the Subprocessor List under contractual data protection obligations.

Prohibited Data is out of scope. DeployReady does not classify, process, or hold Federal Contract Information (FCI), Controlled Unclassified Information (CUI), Classified National Security Information, ITAR-controlled data, EAR export-controlled data, Protected Health Information (PHI), or any data subject to DFARS 252.204-7012. These categories are Prohibited Data under the Terms of Service. Customers warrant that they will not upload Prohibited Data. If Prohibited Data is inadvertently received, Capstone will notify the customer and delete it.

4. Data in Transit

All data transmitted between customer browsers and `app.capstonehorizon.com` is encrypted using TLS 1.2 or higher, enforced at the Railway HTTPS ingress layer. All API calls from the DeployReady application to subprocessors (OpenAI, Anthropic, xAI, Stripe, Resend, Railway Postgres) use TLS for transport. There is no unencrypted HTTP path to customer data.

5. Data at Rest

Customer data is stored in a Railway-managed Postgres database. Railway applies AES-256 encryption at rest as a default. The encryption key lifecycle is managed by Railway's infrastructure layer, which inherits AWS KMS practices for the us-east-1 region. Capstone does not hold or manage raw encryption keys.

6. Access Control

Application layer: Every request to a data-bearing API endpoint is gated by a valid server-side session. The session includes a `tenantId` that is bound to the request object at authentication time. Every database query that reads or writes Tenant Data includes a `WHERE tenant_id = req.tenantId` condition enforced in application code.

Database layer: Postgres Row-Level Security policies (policy name: `tenant_isolation`) are applied at database startup on 19 tenant-scoped tables. These policies enforce `current_setting('app.tenant_id')` filtering at the database level, independent of application-layer logic. RLS enforcement depends on the database role having sufficient permissions; current production state should be verified using the `scripts/verify-rls.ts` utility.

Administrative access: Capstone engineering access to the production database is through Railway's access controls. All such access is logged.

Role-based permissions: Within a tenant organization, users hold one of three roles (owner, admin, member). Role is checked at the route level to limit access to privileged operations such as user management and data export.

7. Retention

Data Category	Retention Period	Basis
Solicitation data	12 months from last activity on the solicitation	Operational
Generated proposals	Until the tenant deletes them or terminates the account	Customer control
Company profile and credentials	Duration of active subscription, then 30 days post-termination	Contractual
Audit logs	24 months from event date	Security / compliance
Billing records	Per Stripe's retention practices; minimum 7 years for tax/IRS purposes	Legal
Usage and error logs	90 days	Operational

Capstone does not retain LLM prompt content submitted to OpenAI, Anthropic, or xAI beyond what those providers require for their own API operations. See each provider's API data use policy for their retention terms.

8. Data Deletion

Tenant-initiated deletion: Customers may request full deletion of their Tenant Data at any time by submitting a written request to privacy@capstonehorizon.com. Capstone will process the deletion within 30 days of receiving the request. Deletion cascades to all tenant-scoped tables.

Exceptions to deletion: Audit log entries are preserved after tenant data deletion to maintain the integrity of the security audit trail. Billing records required by law or Stripe's retention policy are also preserved.

Account termination: Upon account termination (by either party), Capstone will delete active Tenant Data within 30 days. The customer will receive written confirmation of deletion.

9. Data Location

All DeployReady customer data is stored in the United States, in AWS us-east-1 (Northern Virginia). Capstone does not currently transfer customer data outside the United States. If this changes, Capstone will notify customers and update this policy at least 30 days in advance.

10. Backups

Railway performs automated daily snapshots of the Postgres database. Snapshots are retained for 7 days, after which they are automatically deleted by Railway. Backups are encrypted at rest using the same AES-256 controls as the live database. Capstone does not maintain separate off-site backups outside of Railway's snapshot infrastructure.

11. Breach Notification

In the event of a confirmed security incident involving unauthorized access to or exposure of Tenant Data:

1. Capstone will notify affected tenants within 72 hours of confirming the breach. The initial notification will include the nature of the incident, data categories involved, and immediate steps taken.
2. Capstone will log the incident and notification in the `audit_logs` table at security@capstonehorizon.com.
3. A written summary of the incident, timeline, impact, and remediation steps will be provided to affected tenants within 5 business days of resolution.
4. If the incident involves personally identifiable information, Capstone will assess state attorney general notification requirements under applicable state breach notification laws and comply accordingly.
5. Capstone will maintain an internal post-mortem record per the Incident Response Plan.

12. Changes to This Policy

Capstone will provide at least 30 days' notice of material changes to this policy via email to the account owner on file and via a notice at capstonehorizon.com/legal/data-handling-policy. Continued use of the service after the notice period constitutes acceptance of the revised policy.

Contact

- Security incidents: security@capstonehorizon.com
- Privacy and data requests: privacy@capstonehorizon.com
- Mailing address: Capstone Horizon LLC, 7782 Rose Rock Way, Las Vegas, NV 89113