DeployReady Incident Response Plan

Effective Date: April 22, 2026
Version: v1.0.0
Last Updated: April 22, 2026
Classification: Internal -- available to enterprise customers and APEX advisors on request
Owner: David Diaz, Founder/CEO (security@capstonehorizon.com)

> *Customer-facing commitments in this document are marked with [CUSTOMER COMMITMENT]. These represent binding obligations that mirror those in our Terms of Service, Data Handling Policy, and DPA Template.*

1. Purpose

This runbook defines how Capstone Horizon LLC ("Capstone") responds to security incidents affecting the DeployReady platform. Its goals are:

1. Detect and contain incidents quickly.
2. Protect customer data and platform integrity.
3. Communicate honestly and promptly with affected customers.
4. Learn from incidents to reduce recurrence.

This document applies to all Capstone personnel, contractors, and subprocessors acting on behalf of Capstone.

2. Scope: What Counts as an Incident

An "incident" is any confirmed or suspected event that compromises or threatens to compromise the confidentiality, integrity, or availability of DeployReady systems or customer data. Incidents include:

Type	Examples
Unauthorized access	Successful credential stuffing, session hijacking, tenant isolation bypass, unauthorized admin access
Data exposure	Customer data visible to wrong tenant, accidental public exposure, subprocessor breach affecting our data
Service disruption	Application unavailability exceeding 1 hour due to a security-related cause (DDoS, infrastructure compromise, ransomware)
Malicious code	Malware deployed in the application stack or on any system handling customer data
Lost or compromised device	Any device with access to production credentials or customer data is lost, stolen, or compromised

Type	Examples
Subprocessor incident	Railway, OpenAI, Anthropic, xAI, Stripe, or Resend reports a security event affecting Capstone customer data

Events that do NOT constitute incidents: routine application errors, failed login attempts within normal threshold, planned maintenance windows.

3. Severity Tiers

Tier	Definition	Initial Response SLA
Sev1	Confirmed or strongly suspected unauthorized access to or exposure of customer data (any amount). Includes subprocessor Breaches affecting our data.	Incident Commander engaged within 1 hour of detection
Sev2	Internal data exposure (no customer data involved), platform service disruption exceeding 1 hour (security-related), or compromised device with production access.	Incident Commander engaged within 4 hours of detection
Sev3	Security misconfiguration with no confirmed data exposure, vulnerability discovered but not yet exploited, failed attack with no compromise.	Reviewed within 1 business day; remediation plan within 5 business days

4. Roles and Responsibilities

Role	Default Holder	Responsibilities
Incident Commander (IC)	David Diaz (Founder/CEO)	Overall incident ownership. Declares severity. Makes final decisions on containment, notification, and escalation. Available 24/7 for Sev1.
Technical Lead	Capstone engineering lead on duty	Leads detection, analysis, containment, and eradication activities. Provides technical briefings to IC.

Role	Default Holder	Responsibilities
Communications Lead	David Diaz (default; may delegate)	Owns all customer-facing communications. Drafts notifications. Updates status page. Handles press inquiries (none expected, but documented).
Backup IC	Designated by David Diaz in writing at each annual review	Assumes IC duties if David Diaz is unavailable.

All role assignments are documented in a separate access-controlled roster. IC designates a backup before taking any planned absence of more than 3 consecutive days.

---

5. Incident Response Phases

Phase 1: Detect

Sources of detection:

- Application monitoring and error logs in Railway
- `audit_logs` table anomaly review (unusual action patterns, failed logins above threshold)
- Customer report to security@capstonehorizon.com
- Subprocessor notification
- External vulnerability disclosure
- Capstone personnel observation

Action: Any person who detects or suspects an incident contacts the Incident Commander immediately via direct message and email to security@capstonehorizon.com. Do not attempt to investigate or contain without notifying the IC first.

Phase 2: Triage

Within 1 hour (Sev1) or 4 hours (Sev2) of detection:

1. IC convenes the response team via secure channel.
2. Technical Lead assesses: Is this a confirmed incident or a false positive?
3. IC declares severity tier.
4. IC creates a private incident record (date, time, reporter, initial facts, severity declaration).
5. Team establishes a dedicated secure communication channel (separate from normal channels) for the incident.

Key triage questions:

- Is customer data confirmed or suspected to be involved?
- Which tenants are affected?
- What is the blast radius?
- Is the attack or exposure ongoing?

- Which systems and subprocessors are involved?

Phase 3: Contain

Objective: Stop the bleeding. Prevent additional data exposure or damage.

Containment actions (select as applicable based on incident type):

- Revoke compromised credentials or API keys immediately.
- Disable affected user accounts or tenant access.
- If a Sev1 is in progress: consider taking the application offline or blocking the source IP/range at Railway.
- Notify affected subprocessors if their systems are involved.
- Preserve all relevant logs before any system changes (Railway logs, audit_logs, session records).
- Do NOT delete or modify logs during or after an incident without IC authorization.

Phase 4: Eradicate

Objective: Remove the root cause.

1. Technical Lead identifies the root cause (e.g., compromised credential, misconfiguration, vulnerability in dependency).
2. Implement the fix in a staged environment where possible; validate before deploying to production.
3. If the fix requires a dependency update or code change, complete it with standard PR review and deploy via Railway.
4. Confirm that the vulnerability or exposure path is closed.

Phase 5: Recover

Objective: Restore normal service safely.

1. Restore any affected systems from clean state (Railway snapshot if data integrity is in question).
2. Confirm tenant isolation is intact via `scripts/verify-rls.ts` and manual audit log review.
3. Re-enable any access or services suspended during containment.
4. Monitor closely for 24 hours post-recovery for signs of recurrence.
5. IC declares incident Resolved.

Phase 6: Post-Mortem

[CUSTOMER COMMITMENT] A written post-mortem will be completed within 10 business days of the Resolved declaration for any Sev1 or Sev2 incident.

Post-mortem contents:

- Timeline (Detection, Triage, Contain, Eradicate, Recover -- with timestamps)
- Root cause
- Customer impact (number of tenants, data categories involved, duration of exposure)
- What went well
- What went wrong

- Action items with owners and target dates
- Lessons learned

Post-mortems are stored in the internal incident record and are available to affected customers on request.

6. Customer Notification SLAs

[CUSTOMER COMMITMENT]

Milestone	Commitment
Initial notification to affected tenants	Within 72 hours of confirming a Sev1 Breach involving customer data
Status page updates during active Sev1	Every 4 hours while the incident is active
Final written incident notification	Within 5 business days of the Resolved declaration
Post-mortem available on request	Within 10 business days of Resolved

Initial notifications are sent from security@capstonehorizon.com to the account owner email address on file for each affected tenant.

7. Regulatory Notification

State breach notification laws. If a Sev1 incident involves personally identifiable information of residents of states with breach notification requirements (all 50 states have such laws), Capstone will assess notification obligations under each applicable state statute and comply accordingly. The Communications Lead owns this assessment. Legal counsel is consulted for any incident involving 500 or more affected individuals, or involving payment card or Social Security numbers.

Federal notification. DeployReady does not process FCI or CUI. No FAR 52.204-21 incident reporting obligation applies. If Capstone is later engaged under a contract that includes FAR 52.204-21 as a flow-down clause (Path A), this plan will be updated accordingly.

FedRAMP / FISMA. Not applicable at current posture.

8. Communication Templates

Template A: Initial Notification (Sev1, sent within 72 hours)

Subject: [DeployReady Security Notice] Security Incident Affecting Your Account

Dear [Account Owner Name],

We are writing to inform you that Capstone Horizon LLC has confirmed a security incident affecting the DeployReady platform that may have involved your account data.

What happened: [Plain-language description -- 2-3 sentences. What type of incident, when it was detected, when it was confirmed.]

What data was involved: [List categories -- e.g., company profile data, solicitation uploads, account email addresses. Be specific about what is confirmed and what is still under investigation.]

What we have done: [Actions taken: containment steps, fix deployed, access revoked, etc.]

What you should do: [Specific recommended actions -- e.g., change your password, review your audit log, contact us if you see unauthorized activity.]

We take this seriously and are working to provide you a full account of the incident. We will follow up with a written summary within 5 business days of resolving the incident.

If you have questions, contact us at security@capstonehorizon.com.

Sincerely,
David Diaz
Founder/CEO, Capstone Horizon LLC
security@capstonehorizon.com

Template B: Final Incident Notification (within 5 business days of Resolved)

Subject: [DeployReady Security Notice] Final Incident Report -- [Incident ID]

Dear [Account Owner Name],

This is our final written notification regarding the security incident we reported on [initial notification date].

Incident summary: [2-3 sentences.]

Root cause: [Plain-language description.]

Data confirmed affected: [Specific categories, approximate record counts if known, duration of exposure.]

Tenants affected: [State whether it was isolated to their account or affected multiple tenants -- without naming other tenants.]

Remediation steps completed: [List actions -- patch deployed at [date], access revoked, RLS confirmed, etc.]

What we are doing to prevent recurrence: [Action items from post-mortem, with target dates.]

Regulatory note: [If applicable: "We have assessed our notification obligations under [State] law and [have notified / are in the process of notifying] the relevant state attorney general."]

If you have further questions or wish to request the post-mortem report, contact security@capstonehorizon.com.

Sincerely,
David Diaz
Founder/CEO, Capstone Horizon LLC
security@capstonehorizon.com

9. Tabletop Exercise Cadence

[CUSTOMER COMMITMENT] Capstone will conduct tabletop incident response exercises on the following schedule:

Exercise	Target Date	Scope
Initial tabletop (external facilitation optional)	Q3 2026	Walk through Sev1 scenario (tenant isolation bypass, customer data exposure). Produce written exercise report.
Second tabletop	Q1 2027	Subprocessor breach scenario (Railway or LLM API provider). Update plan based on Q3 2026 lessons.
Ongoing quarterly reviews	Q3 2026 onward	Review this plan for currency; update roles, contacts, and technical procedures.

Written exercise reports are available to enterprise customers and APEX advisors on request.

Contact

Incident reports and security inquiries: security@capstonehorizon.com
Capstone Horizon LLC, 7782 Rose Rock Way, Las Vegas, NV 89113