Incident Response Plan

Version 1.0
May 2026

Amazon Ads API Data Security | Hive Mind Nestor Private Limited

1. PURPOSE & SCOPE

This Incident Response Plan (IRP) defines the procedures Hive Mind Nestor Private Limited follows to detect, contain, eradicate, and recover from any security incident involving data accessed through the Amazon Ads API. It applies to all systems, personnel, and third-party integrations that handle Amazon advertiser data.

2. ASSETS IN SCOPE

- Amazon Ads API credentials (Client ID, Client Secret, Refresh Tokens)
- Advertiser account data: campaign metrics, spend data, ASIN performance
- Brand Analytics report data processed on behalf of authorised sellers
- Application servers: optimizer.hivemindnestor.com (Railway, US region)
- JWT session tokens for authenticated users
- Environment variable stores containing API secrets

3. INCIDENT CLASSIFICATION

Priority	Category	Example	Response SLA
P1 Critical	Confirmed breach	Unauthorised access to advertiser data	2 hours
P2 High	Suspected breach	API credential exposure or anomalous API calls	4 hours
P3 Medium	Policy violation	Internal misuse of data outside stated purpose	24 hours
P4 Low	Near-miss	Failed intrusion attempt with no data exposure	72 hours

4. RESPONSE TEAM

Hive Mind Nestor operates as a lean organisation. The Founder serves as the sole Incident Commander with direct accountability for all security decisions.

Role	Name	Contact	Responsibility
Incident Commander	Fasihuddin Ahmer	info@hivemindnestor.com	All P1/P2 decisions, Amazon notification
Technical Lead	Fasihuddin Ahmer	info@hivemindnestor.com	Credential revocation, system isolation
Client Liaison	Fasihuddin Ahmer	info@hivemindnestor.com	Notify affected advertisers

5. RESPONSE PROCEDURE

Step 1 — Detect & Identify (0–2 hrs)

Monitor Railway logs and API gateway for anomalous patterns. Review Amazon Ads API error rates in the developer dashboard. Identify affected accounts, data types exposed, and attack vector. Document initial findings with timestamps.

Step 2 — Contain (2–4 hrs)

Immediately revoke compromised API credentials via the Amazon Ads developer console. Disable affected Railway service if necessary. Rotate all JWT signing secrets. Block suspicious IP addresses at the network level. Preserve logs for forensic review.

Step 3 — Report to Amazon (within 24 hrs of detection)

Submit incident report to Amazon Ads via the partner support portal. Include: nature of incident, data types affected, number of advertisers impacted, containment actions taken, and remediation timeline. Reference Case format: Amazon Ads API Security Incident — [Date].

Step 4 — Notify Affected Advertisers (within 48 hrs)

Contact all advertisers whose data may have been exposed. Provide: what happened, what data was involved, what actions have been taken, and what advertisers should do (e.g., review campaign activity, change passwords).

Step 5 — Eradicate & Recover (24–72 hrs)

Remove malicious access, patch vulnerabilities, re-issue all API credentials, redeploy clean application build. Verify system integrity before restoring advertiser connections. Confirm with Amazon that new credentials are active.

Step 6 — Post-Incident Review (within 7 days)

Conduct root cause analysis. Update security controls to prevent recurrence. Document lessons learned. Update this IRP if procedures proved inadequate. File final incident report internally and share summary with Amazon if requested.

6. AMAZON REPORTING REQUIREMENT

Per the Amazon Ads Data Protection Policy, Hive Mind Nestor will report all P1 and P2 security incidents to Amazon within **24 hours of detection**.

Reporting Channel	Details
Partner Support Portal	advertising.amazon.com → Support → Contact Us
Subject Line Format	SECURITY INCIDENT — Hive Mind Nestor — [YYYY-MM-DD]
Minimum Information	Incident type, affected data, advertisers impacted, actions taken
Follow-up	Final report within 7 days of incident closure

7. CURRENT TECHNICAL CONTROLS

- All Amazon Ads API credentials stored as encrypted environment variables in Railway — never in source code or version control
- HTTPS enforced on all application endpoints (optimizer.hivemindnestor.com)
- JWT-based authentication required on all /api/* routes
- Auth middleware gates all tenant-scoped brand analytics endpoints (confirmed 401 on unauthenticated requests)
- API credentials rotated regularly and immediately upon any suspected exposure

- Access to production systems restricted to authorised personnel only
- No advertiser PII retained beyond the active authenticated session
- Source code maintained in private repository with access controls
- Railway deployment logs retained for 30 days for forensic purposes

8. REVIEW & MAINTENANCE

This plan will be reviewed and updated: (a) annually, (b) following any security incident, (c) upon significant changes to the application architecture or Amazon Ads API integration, or (d) upon request from Amazon.

AUTHORISATION

Authorised Signatory	Organisation	Date
Fasihuddin Ahmer	**Hive Mind Nestor Private Limited**	**May 2026**
Founder & Managing Director	CIN: U74999UP2019PTC114XXX	
info@hivemindnestor.com	hivemindnestor.com	