Security Incident Reporting Procedure

Version 1.0
May 2026

Amazon Ads API Compliance | Hive Mind Nestor Private Limited

1. PURPOSE

This document defines the Security Incident Reporting Procedure for Hive Mind Nestor Private Limited in its capacity as an Amazon Ads Verified Partner. It ensures that all security incidents involving Amazon Ads API data are reported to Amazon promptly, accurately, and in the format required by the Amazon Ads Data Protection Policy (DPP).

2. SCOPE

This procedure applies to all security incidents that involve or may involve data obtained via the Amazon Ads API, including but not limited to:

- Unauthorised access to Amazon Ads API credentials or tokens
- Exposure or suspected exposure of advertiser campaign data
- Anomalous API call patterns suggesting credential misuse
- Third-party breach affecting systems that store Amazon Ads data
- Internal policy violations relating to Amazon data handling
- Loss or theft of devices containing Amazon Ads API access credentials

3. REPORTING TIMELINES

Incident Priority	Internal Escalation	Amazon Notification	Final Report
P1 — Critical	Immediate	Within 24 hours	Within 7 days
P2 — High	Within 1 hr	Within 24 hours	Within 7 days
P3 — Medium	Within 4 hrs	Within 72 hours	Within 14 days
P4 — Low	Within 24 hrs	Optional	Within 30 days

4. HOW TO REPORT TO AMAZON

Step 1 — Gather Required Information

- Date and time of incident detection
- Nature of the incident (breach, suspected exposure, misuse)
- Amazon Ads API application ID affected
- Data types involved (campaign data, advertiser IDs, API tokens)
- Estimated number of advertisers impacted
- Containment actions already taken
- Current status (ongoing / contained)

Step 2 — Submit via Amazon Partner Support

Portal URL	advertising.amazon.com → Help → Contact Us → API Support
Subject Line	SECURITY INCIDENT — Hive Mind Nestor — [YYYY-MM-DD]
Case Type	Data Security / Policy Compliance
Include	All information gathered in Step 1 plus any log excerpts
Attach	Incident timeline document (internal incident log)

Step 3 — Follow Up

Respond to any Amazon follow-up requests within 24 hours. Provide a final incident closure report within the timeline specified in Section 3, including root cause analysis and remediation actions taken.

5. INTERNAL ESCALATION PATH

All incidents, regardless of priority, must be escalated to the Incident Commander immediately upon detection. Do not attempt to resolve a P1 or P2 incident without notifying the Incident Commander first.

Role	Person	Contact	When to Escalate
Incident Commander	Fasihuddin Ahmer	info@hivemindnestor.com +91-XXXXXXXXXX	All incidents immediately
Amazon Ads Support	Amazon Team	advertising.amazon.com/support	P1/P2 within 24 hours

6. WHAT NOT TO DO DURING AN INCIDENT

- Do NOT attempt to cover up or delay reporting a confirmed breach
- Do NOT continue using compromised API credentials — revoke immediately
- Do NOT delete logs or evidence before forensic review
- Do NOT notify external parties (press, social media) before Amazon notification
- Do NOT re-use rotated credentials or tokens
- Do NOT handle a P1/P2 incident alone — escalate first

7. PREVENTIVE CONTROLS CURRENTLY IN PLACE

The following controls reduce the likelihood of a reportable incident:

Credential Storage	All API keys stored as Railway environment variables — never in code
Encryption in Transit	HTTPS enforced on all endpoints via Railway TLS termination
Authentication	JWT auth middleware on all API routes (401 on unauthenticated access)
Access Control	Tenant-scoped endpoints — each org sees only its own data
Token Rotation	API tokens rotated upon any suspected exposure or staff change
Data Minimisation	No advertiser PII stored beyond the active session
Log Retention	Railway deployment and access logs retained for 30 days
Source Control	Private repository with branch protection and access controls

8. DOCUMENT CONTROL

Document Title	Security Incident Reporting Procedure
Version	1.0
Effective Date	May 2026
Review Cycle	Annual or following any security incident
Owner	Fasihuddin Ahmer, Founder — Hive Mind Nestor Private Limited
Related Documents	Incident Response Plan v1.0

AUTHORISATION

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