Incident Response Policy

Dash Media Limited · Version 1.1 · Effective 28 October 2026 · Review by 28 October 2027 · Owner: Brad Hook, Director, Dash Media Limited

1. Purpose

To define what counts as a security incident, how we respond, and when and how we tell affected clients and participants.

2. What counts as an incident

- Unauthorized access to, or disclosure of, participant or client data
- Loss or corruption of participant data
- Compromise of an administrative account, credential, or API key
- A vulnerability that could allow any of the above, whether or not it was exploited
- A security incident at a subprocessor that affects our data
- Sustained loss of availability of a product

Suspected incidents are treated as incidents until shown otherwise.

3. How to report

- **Clients, participants, researchers:** email hello@flame.live. Include what you saw, where, and when.
- **Automated alerts:** Supabase and Vercel send email alerts for unusual activity and failed deployments to the Director. GitHub sends Dependabot alerts.

We acknowledge external reports within one business day.

4. Response steps

1. Contain (hours 0 to 4). Stop the exposure: rotate the affected credential, disable the affected account or route, roll back the deployment, or take the product offline if needed. Containment comes before investigation.

2. Assess (hours 4 to 24). Establish what data was affected, how many people, over what period, and whether it is still exposed. Preserve logs from Vercel, Supabase, and GitHub. Record a timeline as it is discovered.

3. Notify (within 72 hours of confirming a breach, sooner where required). See section 5.

4. Remediate. Fix the root cause, not only the symptom. Verify the fix on a preview deployment before production.

5. Review (within 14 days). Write a short post-incident report: what happened, timeline, impact, root cause, what changed, and what would have caught it earlier. Update policies and controls accordingly. Share the report with affected clients on request.

5. Notification

WHO	WHEN	HOW
Affected clients	Within 72 hours of confirming that their participants' data was affected; earlier if the client's contract specifies	Email to the client's named contact, followed by a call if the impact is material
Affected participants	Where the client agrees or where the law requires, within the same window	Email, with plain-language description of what happened and what they should do
New Zealand Office of the Privacy Commissioner	For a notifiable privacy breach under the Privacy Act 2020 (serious harm likely), as soon as practicable	Via the Commissioner's online form
Other regulators	Where a client's jurisdiction requires (for example GDPR 72-hour rule)	In coordination with the client as controller

Notifications include: what happened, what data was involved, what we have done, what the recipient can do, and a contact for questions. We don't delay notification to make the news sound better.

6. Subprocessor incidents

If Vercel, Supabase, GitHub, Anthropic, or another subprocessor notifies us of an incident affecting our data, the steps above apply from the point of notification. We check each subprocessor's status page and security notices during any incident investigation.

7. Contacts

ROLE	PERSON
Incident lead	Brad Hook, Director
Backup contact	Evgeniya Ignatova, Programme Management, FLAME, geniya@bradleyhook.com

8. Testing

The response steps are walked through annually against a hypothetical scenario (for example, a leaked API key) and the policy updated with what was learned.

9. Review

Reviewed annually and after every incident.

10. Version history

VERSION	DATE	CHANGE
1.0	2026-10-27	Initial publication