NUCLEUSLINKS
RTB Network Compliance Policy
Click URL & Landing Accuracy

Effective Date: May 31, 2026

Document Version	Effective Date	Applies To
V2.0	May 31, 2026	All RTB Network Partners

1. Context — Why This Policy Exists

Nucleuslinks is committed to delivering a seamless, trustworthy experience for end users across all publisher surfaces. Our RTB ecosystem connects advertisers, networks, and publishers — and the integrity of that connection depends on users landing exactly where they are intended to land.

1.1 The Problem We Are Solving

Today, there is no validation layer that ensures a Click URL returned by an RTB network actually delivers the user to the correct Brand Domain or product page. This creates three critical risks:

- User Experience Degradation: Users clicking on an ad for Nike land on an unrelated page, damaging trust in both the publisher and the advertiser.
- Advertiser Fraud Exposure: Advertisers pay for clicks expecting users to reach their declared landing page. Misdirected traffic means advertisers pay for zero-value impressions.
- **Publisher Reputation Risk:** When a user clicks and lands on an incorrect or irrelevant destination, it directly damages the publisher's credibility. This impact is consistent across all publishers — whether operating via Network+ (N+) relationships or direct network integrations — as the end user associates the poor experience with the publisher's platform.

1.2 The Role of Deeplink Declaration

A deeplink is the specific URL that takes a user to a precise product page, category, or section within a brand's app or website — as opposed to the generic homepage. When an RTB network wins a bid, Nucleuslinks needs confidence that:

- The Click URL lands on the exact Brand Domain declared in the request.
- If a deeplink was provided in the request, the user arrives at that specific page — not a generic homepage.
- If no deeplink was provided, the user lands on the brand's homepage, correctly derived from the Brand Domain.

Policy Objective: To ensure every Click URL returned in an RTB bid response correctly and verifiably lands the user on the declared Brand Domain and Deeplink (where applicable).

Networks must declare their final landing behaviour in each bid response, and Nucleuslinks will validate this in real-time. Non-compliant responses will be rejected.

2. Technical Guide — Compliance Implementation

This section defines the updated RTB request and response schema, landing rules, and validation logic that all Nucleuslinks RTB network partners must comply with effective May 31, 2026.

2.1 How RTB Requests Currently Work

Every RTB bid request sent by Nucleuslinks includes the following parameters:

Parameter	Description / Behaviour
Brand Domain	Always included. Mandatory. Identifies the advertiser's root domain.
Deeplink	Optional. May contain: a deeplink URL, a homepage URL, or be left empty (homepage is then inferred from the brand domain).

RTB responses currently include only: Click URL and Bid Value. There is no strict validation currently in place for landing accuracy.

2.2 New Request Parameters (Nucleuslinks Will Include)

From the effective date, Nucleuslinks will pass two additional parameters in every RTB bid request:

Parameter	Values	Description
&strict_landing=	1 or 0	Controls the degree of landing match required (see 2.4 for full rules).
&test_click=	1 or 0	1 = Test/Audit request. Not for revenue generation, but a valid ad response is still expected. 0 = Normal live traffic.

2.3 New Response Parameter (Networks Must Return)

In addition to Click URL and Bid Value, all bid responses must include:

Parameter	Description
&final_url=	The final landing URL after all redirects have fully resolved. Must belong to the same brand as brand_domain.

2.4 Landing & Response Rules

Landing behaviour is governed by the strict_landing flag passed in the request.

Strict_landing = 1 (Strict Enforcement)

- Networks must ensure that the user lands on the exact domain passed in the deeplink parameter.
- Any redirection initiated by the brand (e.g., geo-based domain change) is acceptable.

Strict_landing = 0 (Flexible Enforcement)

- Networks must ensure that the user lands on the correct brand domain, even if it is not the exact domain passed.
- All redirects must remain within the same brand domain; cross-brand or irrelevant geo redirections are not permitted.

2.5 Nucleuslinks Validation Logic

Nucleuslinks will run real-time validation on every bid response. The logic differs by strict_landing mode:

A. When strict_landing = 1

Condition	Outcome
final_url exactly matches deeplink (if present)	☑ ACCEPTED — Eligible for serving
domain from final_url matches brand_domain (if deeplink is empty)	☑ ACCEPTED — Eligible for serving
Any mismatch from declared value	✗ REJECTED — Not eligible for serving

B. When strict_landing = 0

Condition	Outcome
final_url belongs to same brand and is geo-relevant	☑ ACCEPTED — Eligible for serving
Cross-brand redirect detected	✗ REJECTED — Not eligible for serving
Geo-irrelevant domain (e.g., nike.fr for IN user)	✗ REJECTED — Not eligible for serving

2.6 Use Case Examples

strict_landing = 1 — Exact Match Required

Case	Geo	Brand Domain	Deeplink (&d=)	Final URL	Result

1	IN	nike.com	(empty)	nike.com	☑ Valid
2	UK	nike.com	https://nike.com	https://nike.com	☑ Valid
3	US	nike.com	https://nike.com/shoes/running	https://nike.com/shoes/running	☑ Valid
4	IN	nike.com	(empty)	nike.in	✗ Invalid
5	UK	nike.com	https://nike.com	https://nike.co.uk	✗ Invalid
6	US	nike.com	https://nike.com/shoes/running	https://nike.com/shoes	✗ Invalid
7	IN	nike.com	https://nike.com/shoes/running	https://nike.in/shoes/running	✗ Invalid

strict_landing = 0 — Geo-Relevant Same-Brand Landing Required

Case	Geo	Brand Domain	Input URL (&d=)	Expected Response URL	Result
1	UK	nike.com	(empty)	nike.com / nike.co.uk	☑ Valid
2	UK	nike.com	https://nike.com	nike.com / nike.co.uk	☑ Valid
3	UK	nike.com	https://nike.com/shoes/running	nike.com/shoes, nike.co.uk/shoes	☑ Valid
4	UK	nike.com	https://nike.com/shoes/running	nike.in/shoes	✗ Invalid
5	IN	nike.com	(empty)	nike.in	☑ Valid
6	IN	nike.com	https://nike.com	nike.in	☑ Valid
7	IN	nike.com	https://nike.com/shoes/running	nike.in/shoes/running	☑ Valid
8	Any	nike.com	https://nike.com/shoes/running	adidas.com/shoes	✗ Invalid

2.7 What Networks Need to Update

To become compliant before the May 31, 2026 effective date, networks must:

- Update redirect logic to meet strict or flexible landing requirements as signalled per request.
- Update bid response schema to include &final_url= in every response.
- Implement no-ad response logic for strict_landing = 1 cases where exact landing cannot be guaranteed.
- Ensure &test_link= requests are handled correctly: return a valid ad response but do not count for revenue.
- Test all redirect chains — including sub-networks and third-party partners — to confirm accurate final landing.

2.8 Tracking & Monitoring

- All mismatches and failures will be logged with timestamp, network ID, request ID, declared vs actual landing URL.
- Rejection rates will be tracked per network and per publisher for auditing and partner quality evaluation.
- Networks may request access to their own mismatch logs for debugging purposes.

3. Breach Policy & Enforcement

Nucleuslinks operates a strict, zero-tolerance policy for landing misdirection. Any confirmed instance where a user is redirected to a domain other than the declared Brand Domain constitutes a breach.

3.1 What Constitutes a Breach

A breach is confirmed when Nucleuslinks' validation system detects that the final landing domain delivered to the user does not match the Brand Domain declared in the bid request. This includes:

- Landing on a different brand's domain entirely.
- Landing on an unrelated third-party or intermediate redirect page.
- Landing on a parked domain, error page, or non-functional URL.
- Any redirect chain manipulation that alters the final destination after bid acceptance.

3.2 Applies To: Network+ (N+) and Non-N+ Publishers

Scope of Enforcement: This policy applies universally across all RTB network partners, regardless of publisher type. Both Network+ (N+) publishers and Non-Network+ publishers are subject to the same breach detection, enforcement timeline, and escalation rules described in this section.

3.3 First & Second Breach — Immediate Response Protocol

Upon detection of a breach (first or second occurrence for a given publisher):

Step	Action	Detail
1	Immediate Deactivation	The network is made inactive immediately upon breach confirmation. All traffic to the network is halted with no grace period.
2	48-Hour Fix Window	The network is given 48 hours to investigate, resolve the root cause, and notify Nucleuslinks that the fix has been deployed. No traffic will be restored during this window.
3	48-Hour Review & Testing	Once fix notification is received, Nucleuslinks takes up to 48 hours to independently review and test the network's redirect behaviour.

4	Controlled Reinstatement	If testing confirms compliance, traffic is re-opened for a limited selection of merchants only. Full traffic restoration is subject to continued monitoring and satisfactory performance.

3.4 Third Breach — Blacklisting

3.5 Blacklist Override — Publisher-Initiated Reinstatement

Reinstatement from a blacklist status is only possible if the publisher explicitly requests it. The reinstatement process requires:

- A formal written request from the publisher to Nucleuslinks confirming they wish to reactivate the network.
- The publisher acknowledges the breach history and accepts responsibility for subsequent compliance.
- Nucleuslinks reserves the right to impose additional conditions, restricted traffic volumes, or enhanced monitoring as part of any reinstatement agreement.
- Reinstatement is not guaranteed and remains at the sole discretion of Nucleuslinks.

This override mechanism exists to respect publisher autonomy — if a publisher has a direct relationship with a network and chooses to reactivate them, Nucleuslinks will facilitate that while maintaining full audit trails.

3.6 Breach Escalation Summary

Breach #	Immediate Action	Resolution Path
1st	Network deactivated immediately	48h fix window → 48h review/testing → Controlled reinstatement (limited merchants)
2nd	Network deactivated immediately	48h fix window → 48h review/testing → Controlled reinstatement (limited merchants)
3rd	Permanent blacklist — all traffic suspended	Reinstatement only possible if publisher explicitly requests reactivation. Subject to Nucleuslinks approval.

4. Responsibility & Liability

Networks are fully and solely responsible for ensuring the user lands on the correct final destination. This responsibility is non-delegable and extends to:

- Any sub-networks or demand-side partners operating within the network's redirect chain.
- Any third-party redirect technologies or tracking solutions introduced by the network.
- Any dynamic redirect logic that varies final destination based on device, geography, or user agent.

Nucleuslinks will not be liable for any costs, lost revenue, or operational impacts associated with non-compliant bid responses. Rejected bids are the sole responsibility of the submitting network.

Questions & Implementation Support: Networks seeking clarification on compliance requirements or needing support with technical implementation should reach out to their Nucleuslinks account manager before the May 31, 2026 effective date. Post-effective-date enforcement will be applied automatically with no exceptions.

Nucleuslinks — Effective May 31, 2026