Creative Compliance Guidelines

These guidelines apply to every creative on the platform that contains third-party code: JavaScript and HTML tags, HTML5 creatives that load external resources, VAST and VPAID tags, and third-party impression and click trackers.

They keep users, publishers and our ad exchange partners safe, and they keep your campaigns eligible for the inventory you buy. Exchanges and publishers enforce their own ad quality rules, and a single non-compliant tag can get a campaign blocked across a whole exchange.

How we check creatives

- We check creative tags with automated scanning and manual review, before campaigns go live and while they run.
- A creative that breaks these guidelines is paused, even if it was approved earlier.
- Any change to a tag, or to what it loads, is checked again.
- Review usually takes up to one business day. Creatives that follow these guidelines are approved fastest.

1. Use recognized sources only

Every script, image, font, video file and tracker in your tag must load over HTTPS from one of these sources:

- the advertiser’s own domains,
- files hosted on the platform and the platform’s macros,
- recognized third-party ad servers and measurement or verification vendors, and
- standard code libraries from established content delivery networks.

This applies to every URL in the tag, including URLs inside click macros or in encoded form. A recognized vendor in your tag does not cover any other host in the same tag. Hosts we cannot verify are held for review and may be rejected.

2. Your tag must show your creative

We need to see and verify the creative behind every tag.

- Tags from a recognized ad server that serve the advertiser’s own creative are accepted.
- Tags that hand the impression to another ad network, exchange or publisher ad server are not accepted. This includes ad network loaders, publisher passbacks and Google Ad Manager (GPT) passback tags.
- The tag must show our reviewers the same creative it shows users. Showing reviewers different content (cloaking) leads to account suspension.
- If your ad server restricts delivery by country or IP address, contact support before launch. We’ll tell you which domain to allow so we can review the creative. Tags we cannot render are rejected.

3. Keep the code transparent

- No obfuscated or encoded code, such as eval or atob calls that hide what the tag does, URLs assembled from fragments, or hidden hosts.
- Minified code is fine. Code written to hide its behavior is not.
- The tag must behave the same way for every viewer and keep the behavior it had when it was approved.

4. Protect user data

- The tag itself must not collect user data: no reading or writing cookies or local storage, no IP address lookups, no device fingerprinting and no collecting browser or location details.
- Only your declared ad server and measurement vendors may collect data, and only to serve and measure this campaign.
- Data passed through the platform’s macros, such as device, site or placement details, may go only to your declared ad server or measurement vendor, for the same purpose.

5. Respect the user’s experience

- No auto-refresh: one impression shows one creative.
- No auto-redirects: users leave the page only when they click.
- No pop-ups, pop-unders, overlays or browser dialogs, and no downloads without a click.
- Sound plays only after the user chooses to play it.
- The creative stays within its declared size. Expanding or floating behavior is allowed only when the creative is set up as a floating ad.
- No fake buttons, fake close buttons or simulated clicks.

6. Clicks and landing pages

- JavaScript banner tags must use the {CLICK_URL} macro for clicks, so every click is counted. Additional click trackers are allowed only from recognized measurement vendors.” This one applies to every creative type.
- The landing page must belong to the advertiser on the account or its brand group. A product page on the brand’s global site is fine; a page for a different brand is not.
- No redirect chains through unrelated domains.
- Landing pages must not impersonate another brand, ask for login or payment details under false pretenses, or start downloads by themselves.
- The landing page must be live and open to our reviewers.

What happens if a creative breaks these guidelines

- The creative or campaign is rejected, with the reason shown in the dashboard.
- Live campaigns that use the creative are paused.
- Serious or repeated breaches lead to account suspension. These include malicious code, collecting user data, cloaking, impersonation and phishing.

These guidelines apply in addition to the terms of service for your account. We may update them as industry standards and our partners’ requirements change.

Revision #7
Created 9 October 2026 07:04:32 by Roberta Karpoviciute
Updated 27 October 2026 15:13:30 by Roberta Karpoviciute