Minimum Traffic Standards &

Compliance Requirements for Publishers

To ensure high-quality traffic and maintain a transparent, fraud-free advertising ecosystem, all **partners and publishers** working with PPCmate must adhere to the following standards:

1. Traffic Source & Content Quality

1. **No Adult Traffic** – Only mainstream, brand-safe traffic is allowed. Any traffic originating from adult, NSFW, or explicit content is strictly prohibited.
2. **No Network-Sourced Traffic** – Traffic must originate from direct placements within the SSP's controlled inventory. Arbitraged, re-brokered, or resold traffic from unknown sources is **not allowed**.
3. **No Iframe Traffic** – All traffic must be fully viewable and not embedded within iframes, popunders, or hidden elements.
4. **No Unknown Devices or Browsers** – Traffic must include a valid and identifiable user-agent. Requests from unknown or spoofed devices and browsers will be rejected.
5. **No Masked or Spoofed Domains** – The SSP must provide real, verifiable domains. Masked, proxied, or spoofed referrer data is strictly prohibited.
6. **No Encrypted or Obfuscated Domains** – Any encrypted, obfuscated, or otherwise unidentifiable domains will not be accepted.
7. **No Numeric or Non-Domain Traffic Sources** – Traffic from non-standard domains, numeric sources (e.g., `00000`, `00036vs`), or untraceable origins is prohibited.

2. Fraud Prevention & Traffic Authenticity

8. **No Incentivized Traffic** – Traffic must be organic and user-driven. Any traffic from incentivized models (e.g., pay-to-click, faucet sites, or rewards programs) is prohibited.
9. **No Proxy, VPN, or Datacenter Traffic** – Traffic must come from genuine end-users. Requests originating from proxy servers, VPNs, or datacenter IPs will be filtered out.
10. **No Bot, Automated, or Non-Human Traffic** – All traffic must be at least **90% human** based on industry-standard fraud detection tools. Suspicious activity will trigger audits.
11. **No Malware, Phishing, or Fraudulent Traffic** – Any traffic from malware-infected sites, phishing sources, or fraudulent placements will result in an immediate partnership suspension.
12. **No Pop-to-Pop Traffic Chaining** – Popunder traffic cannot be further resold into another pop network. Pop-to-pop chaining is strictly forbidden.
13. **No Forced Clicks or Auto-Redirects** – Traffic must originate from genuine user engagement. Auto-redirects, forced clicks, or misleading engagements are not acceptable.
14. **No Excessive Redirects or Cloaking** – The SSP must not use excessive redirects, cloaking, or misrepresentation techniques to disguise traffic sources.

3. Technical Compliance & Filtering Requirements

15. **IP Limit Enforcement (`IPlimit -1`)** – SSPs must ensure that a single IP does not generate excessive requests, preventing artificial traffic inflation.
16. **IP Match Filtering (`Ipmatch Filter`)** – Traffic sources must pass IP verification to prevent spoofing, duplication, or invalid impressions.
17. **Referral Match Filtering (`Referral Match Filter`)** – The SSP must provide valid referral sources. Traffic with fake or missing referrer data will be rejected.
18. **Non-Empty Referrals (`Non Empty Referrals`)** – All traffic must contain a valid and identifiable referrer URL. Empty or null referrer values will not be accepted unless explicitly agreed upon.
19. **Repeated Click Prevention (`Repeated Clicks`)** – Excessive click frequency from the same IP/user will be flagged. SSPs must implement protections against click spamming and artificially inflated CTRs.

4. Performance & Accountability

20. **No Low-Quality Traffic** – SSPs must maintain an acceptable **conversion rate, engagement time, and viewability threshold**. Underperforming sources may be blocked.
21. **Quality Monitoring & Reporting** – The SSP must allow real-time tracking, reporting, and blocking of low-performing or suspicious sources.
22. **Compliance Audits** – PPCmate X reserves the right to conduct periodic audits on SSP partners. Failure to meet standards may result in **traffic filtering, payment holds, or termination**.
23. **Verification & Whitelisting** – New SSP partners must pass an **onboarding verification process** before being fully integrated into PPCmate X.

Enforcement & Penalties

- **Real-Time Traffic Filtering** – Non-compliant traffic will be blocked automatically by PPCmate X's internal anti-fraud systems.
- **Monetization Penalties** – Repeated violations may result in payment reductions or **withheld earnings** for affected traffic.
- **SSP Partnership Termination** – Severe or repeated infractions will lead to an immediate termination of the SSP partnership.