



Clean Play Audit Manual 1.0

Consistent evidence, testing, findings, remediation, decision, surveillance, and renewal

Clean Play Standards

August 6, 2026



Contents at a glance

- 1. Independence and pay-to-pass protection
- 2. Audit stages
- 3. Evidence levels
- 4. Finding severity
- 5. Test protocol
- 6. Decision record
- 7. Material changes
- 8. Complaints and surveillance
- 9. Renewal



Purpose: Consistent, evidence-based assessment of a named mobile game against CPS-MG-1.0.

1. Independence and pay-to-pass protection

- The certification decision is recorded before any maintenance contribution or waiver is requested.
- The \$12 annual certification-maintenance contribution supports registry operation; it is requested after a pass, may be waived, and is not an audit score or guarantee.
- Reviewers disclose conflicts and recuse when they have a financial, employment, family, investment, competitive, or close personal relationship with the applicant.
- Applicants may not select a preferred reviewer solely to obtain a favorable result.

2. Audit stages

1. Intake and identity check.
2. Scope freeze: product, platforms, build numbers, regions, business model, and service inventory.
3. Completeness review.
4. Automated and manual dependency/traffic review where feasible.
5. Representative playthrough and edge-case testing.
6. Evidence review for all nine commitments.
7. Findings report with citations to evidence.
8. Remediation window.
9. Independent decision check.
10. Post-decision contribution or waiver confirmation and credential issuance.
11. Public registry publication and monitoring.

3. Evidence levels

- **E1 - Statement:** Applicant explanation only. Never sufficient for high-risk claims.
- **E2 - Interface evidence:** Screenshots, recordings, store metadata, and settings.
- **E3 - Technical evidence:** Dependency list, config, network records, manifests, data map, server rules, or code excerpts.
- **E4 - Independent reproduction:** Reviewer directly observes the behavior in a supplied build.
- **E5 - External record:** Processor terms, platform records, receipts, public policies, or third-party test results.

A pass normally needs E4 plus E2/E3 for user-visible rules and E3/E5 for data/service claims.

4. Finding severity

- **Critical:** Active paid randomness, material hidden subscription, undisclosed tracking, deceptive forced ad, or intentional badge fraud. Immediate fail or suspension.
- **Major:** A mandatory rule fails in a meaningful user path. No badge until corrected.
- **Minor:** Documentation, labeling, or low-impact implementation gap that could become noncompliant. No final badge until resolved unless the published standard expressly permits a short corrective window.
- **Observation:** Improvement suggestion outside the mandatory nine commitments.

5. Test protocol

CPS-01 - No Disruptive Ads

Pass test: Reviewers can complete a representative play session without receiving a network ad, forced commercial interruption, deceptive ad control, or progress gate tied to advertising.

Reviewer actions: - Test first launch, menus, pause, failure, level transitions, background/return, and offline mode. - Inspect dependency list and network requests for ad/mediation endpoints. - Open every commercial link and record labeling and destination.



CPS-02 - No Tracking

Pass test: Every collected field has a necessary, disclosed purpose; prohibited identifiers and profiling are absent; permitted diagnostics are minimized, secured, and time-limited.

Reviewer actions: - Compare declared data map with observed permissions, manifests, SDKs, and network destinations. - Confirm identifiers, retention, and processor reuse restrictions. - Test deletion/opt-out where applicable.

CPS-03 - No Forced Accounts

Pass test: A reviewer can access the game's basic promised experience without creating an account unless the entire product is inherently account-based and the necessity is documented and accepted in scope.

Reviewer actions: - Install clean and attempt first play without account creation. - Compare guest and account features. - Test account deletion and marketing consent separation.

CPS-04 - No Loot Boxes

Pass test: No payment, paid token, subscription benefit, advertisement, or purchasable accelerator can produce or materially increase a randomized reward.

Reviewer actions: - Trace every purchase, reward, chest, spin, drop, key, pack, and currency conversion. - Attempt to reach random outcomes from paid value or subscription benefits.

CPS-05 - No FOMO Mechanics

Pass test: Taking a normal break does not destroy accumulated value, create a material competitive penalty, or expose the player to deceptive urgency or a monetized wait.

Reviewer actions: - Record timers, streaks, events, offers, daily rewards, and scarcity claims across several dates or test configurations. - Determine the consequence of missing a day or stopping play.

CPS-06 - No Premium Currencies

Pass test: A player can identify the exact real-world price of each purchase at the decision point without converting an in-game currency or consuming a prepaid balance.

Reviewer actions: - List every currency and source. - Verify direct local-currency pricing and absence of paid intermediate value.

CPS-07 - No Pay-to-Win

Pass test: A paying player receives no gameplay advantage over a nonpaying player in shared competition, and no purchase is needed to escape intentionally monetized frustration.

Reviewer actions: - Map every purchase to gameplay effect. - Test competitive and progression impact and inspect frustration-adjacent prompts.

CPS-08 - No Hostile Notifications

Pass test: All nonessential notifications are off until affirmatively enabled, every category can be disabled, and no message uses guilt, deception, or artificial urgency.

Reviewer actions: - Trigger all notification categories in a test account/device. - Verify default state, wording, timing, quiet hours, and disable controls.



CPS-09 - No Hidden Subscriptions

Pass test: A reasonable user can identify the recurring amount and cadence before purchase and reach the platform cancellation control from the app or service without obstruction.

Reviewer actions: - Record purchase disclosure, trial conversion, restore, management, cancellation, and post-cancellation behavior. - Compare prominent price language with actual charge.

6. Decision record

Each decision record contains scope, evidence list, rule-by-rule result, unresolved observations, reviewer, checker, dates, expiry, and credential identifier. Public summaries must not expose private source code, personal information, security secrets, or confidential contracts.

7. Material changes

The credential holder must notify Clean Play within 30 days before or after a material release, and before displaying the badge on that release where practical. Material changes include adding or replacing an ad, analytics, attribution, account, purchase, currency, subscription, notification, social, or data-processing system.

8. Complaints and surveillance

Credible complaints are triaged by severity. Clean Play may request a build, reproduction steps, records, or a written response. Review itself is an internal case state. If leaving a credential Active would materially mislead the public or expose players to plausible harm, the credential is Suspended while the issue is resolved; otherwise the internal review proceeds without inventing another public status.

9. Renewal

Credentials expire after 12 months unless renewed. Renewal requires an updated SDK and purchase inventory, change log, current storefront disclosures, and risk-based retesting.

Formation-stage working material. Adoption, legal review, deployment, staffing, testing, and real records are required before production certification.