INVO NETWORK

ACCEPTABLE USE POLICY

Effective Date: January 1, 2026

This Acceptable Use Policy ("AUP") governs the conduct and use of the Invo Network platform (the "Service") by all users, including Players, Developers, and any third parties who access or use the Service. This AUP forms part of the INVO Policies and is incorporated by reference into the INVO Developer Terms of Service and the INVO Player Terms of Service.

INVO may modify this AUP from time to time. Continued use of the Service after modifications take effect constitutes acceptance of the updated AUP.

Violations of this AUP may result in immediate suspension or termination of access to the Service, reversal of Transactions, withholding of payouts, reporting to authorities, and any other remedy available under the INVO Terms or applicable law.

1. General Principles

1.1 Lawful Use

You may only use the Service for lawful purposes and in compliance with these and all applicable INVO Policies, the INVO Terms, and applicable law in every jurisdiction where you use the Service or where the Service has effects.

1.2 Good Faith

You agree to use the Service in good faith, without intent to defraud, deceive, harm, or exploit other users, INVO, or third parties.

1.3 Responsibility

You are responsible for all activity conducted under your account. You must use reasonable security measures to prevent unauthorized access. If you become aware of any unauthorized access or use, you must notify INVO promptly.

1.4 Application

This AUP applies to: (a) Players using the Service to purchase, hold, or use Virtual Currency; (b) Developers integrating with the Service; (c) any persons or entities accessing the Service through APIs, SDKs, dashboards, or other channels; and (d) any content, data, or communications submitted through the Service.

2. Prohibited Activities

You may not use the Service for, or in connection with, any of the following:

2.1 Illegal Activity

- Any activity that violates applicable federal, state, local, or international law
- Money laundering, terrorist financing, or other financial crimes
- Sanctions evasion, including transactions involving OFAC-sanctioned persons, entities, or jurisdictions
- Tax evasion or tax fraud
- Bribery, corruption, or violations of anti-corruption laws
- Human trafficking, forced labor, or modern slavery
- Drug trafficking or sale of controlled substances
- Trafficking in firearms, weapons, or explosives

2.2 Fraud and Deception

- Fraudulent purchases, including use of stolen, fake, or unauthorized payment methods
- Identity fraud, including impersonation of another person, account takeover, or use of false identification
- Chargeback fraud, refund fraud, bonus abuse, or other forms of payment abuse
- Phishing, social engineering, or attempts to deceive other users
- Misrepresentation of Game content, in-Game items, Virtual Currency value, or Service features
- Use of synthetic identities, fake accounts, or coordinated multi-account schemes
- Operating accounts on behalf of others without authorization (account farming or muling)

2.3 Gambling and Wagering

- Unlicensed gambling, lotteries, sweepstakes, or games of chance
- Operating real-money gambling, sports betting, or fantasy sports without all required licenses in every applicable jurisdiction
- Use of Virtual Currency to facilitate gambling outside the supported Game ecosystem
- Skill-based wagering platforms operating in jurisdictions where prohibited

2.4 Cryptocurrency and Decentralized Assets

- Use of the Service to purchase, exchange, receive, or settle cryptocurrency, blockchain-based tokens, NFTs, or any decentralized digital asset
- Operating any product or service involving cryptocurrency, blockchain, decentralized finance (DeFi), or tokenized assets
- Linking the Service to cryptocurrency wallets, exchanges, or blockchain protocols
- Marketing Virtual Currency as a cryptocurrency, token, or investment asset

2.5 Prohibited Products and Content

- Sale or distribution of illegal goods or services
- Sexual content involving minors (CSAM), child grooming material, or any content sexually exploiting children
- Non-consensual sexual content or revenge pornography
- Content promoting terrorism, mass violence, or genocide
- Content promoting hate speech, threats, harassment, or discrimination based on race, religion, ethnicity, national origin, gender, sexual orientation, gender identity, disability, or other protected characteristic
- Content promoting self-harm, suicide, or eating disorders
- Counterfeit goods or content infringing intellectual property rights
- Stolen goods or stolen digital assets
- Adult content unless explicitly approved in writing by INVO and operated in compliance with applicable law

2.6 Harm to Others

- Harassment, threats, stalking, or abusive behavior toward other users or INVO personnel
- Doxing, sharing private information, or violating others' privacy
- Coordinated harassment or brigading
- Content or conduct that endangers minors
- Defamation, libel, or false statements about identifiable persons
- Inciting violence, illegal activity, or harm against others

3. Platform Integrity

You may not engage in any activity that compromises, degrades, or interferes with the Service:

3.1 Unauthorized Access

- Attempting to access any part of the Service without authorization
- Bypassing or attempting to bypass authentication, consent flows, rate limits, or security controls
- Accessing or attempting to access another user's account, balance, or data

- Using stolen, leaked, or unauthorized API keys, credentials, or tokens
- Probing or scanning Service vulnerabilities without prior written authorization from INVO

3.2 Reverse Engineering and Tampering

- Reverse engineering, decompiling, or disassembling the Service, except to the extent expressly permitted by applicable law
- Tampering with, modifying, or interfering with Service components, code, or infrastructure
- Creating derivative works of the Service without authorization
- Attempting to extract, replicate, or substitute the Service or its features

3.3 Automation and Scraping

- Using bots, scripts, scrapers, crawlers, or automated tools to interact with the Service in ways not expressly authorized
- Generating artificial Transactions, automated purchases, or simulated Player activity
- Mass-creating accounts or coordinated multi-account behavior
- Harvesting or collecting data from the Service without explicit authorization

3.4 Service Disruption

- Conducting denial-of-service attacks, distributed denial-of-service attacks, or any other attack designed to disrupt the Service
- Introducing malware, viruses, ransomware, worms, trojans, or other malicious code
- Overloading the Service, consuming excessive resources, or otherwise impairing performance for other users
- Interfering with Service operations, fraud detection, or compliance systems

3.5 Bypassing Consent and Verification

- Bypassing, circumventing, or disabling SMS-based one-time-passcode verification
- Falsifying, forging, or misrepresenting consent records, including phone-share approvals and guardian approvals
- Using fraudulent, fake, or unverified phone numbers or email addresses
- Sharing accounts in ways that defeat consent or verification mechanisms
- Bypassing age verification, parental consent, or guardian approval requirements

3.6 Unauthorized Commercial Use

- Reselling, redistributing, or commercializing access to the Service without authorization
- Using the Service to develop, support, or operate a competing product or service
- Operating account-selling, account-trading, currency-trading, or item-trading platforms outside the Service
- Using the Service in connection with any unauthorized payment aggregation or money services business

4. Financial and Transactional Abuse

4.1 Payment Abuse

- Initiating fraudulent or abusive chargebacks, including "friendly fraud"
- Submitting false or misleading refund requests

- Using payment methods you are not authorized to use
- Layering, structuring, or splitting Transactions to evade limits, taxes, or compliance thresholds
- Manipulating Transaction patterns to obtain bonuses, rewards, or favorable treatment under false pretenses

4.2 Currency and Item Abuse

- Generating, duplicating, or fraudulently obtaining Virtual Currency
- Exploiting bugs, glitches, or unintended Service behavior to obtain Virtual Currency, items, or balances
- Selling, trading, or transferring Virtual Currency or in-Game items outside the Service
- Using third-party services to convert Virtual Currency outside authorized channels
- Using Virtual Currency in ways inconsistent with the supported Games' intended use

4.3 Risk Manipulation

- Concealing or misrepresenting the nature of Transactions
- Misrepresenting Developer business, Game content, or end users to influence risk classification
- Using shell entities or pass-through structures to obscure beneficial ownership
- Operating in industries or with products that violate INVO's risk policies without disclosure

5. Developer-Specific Obligations

In addition to the general prohibitions in this AUP, Developers agree to the following:

5.1 Game Content

- Developers are responsible for all Game content, including content moderation, age-rating compliance, and removal of prohibited content
- Developers must implement reasonable measures to prevent prohibited Player conduct within their Games
- Developers must comply with all applicable consumer protection, advertising, and gaming laws in jurisdictions where the Game is offered

5.2 Faithful Integration

- Implement INVO APIs, SDKs, consent flows, and verification systems as documented
- Not misrepresent INVO Service features, fees, or roles to Players
- Not bypass Platform-side fraud detection, rate limiting, or compliance controls
- Surface required Player notices, including consent requests and verification prompts

5.3 Player Treatment

- Provide reasonable Player support for matters within Developer's control
- Direct Players to INVO support for matters within INVO's control
- Not engage in deceptive marketing, dark patterns, or manipulative monetization tactics, particularly with respect to minors
- Honor refunds and consumer rights as required by applicable law

5.4 Data Handling

- Use Player data only for purposes necessary to operate the Developer's integration
- Comply with all applicable privacy laws, including GDPR, UK GDPR, CCPA, COPPA, and other applicable regulations
- Maintain reasonable data security practices
- Not retain or share Player phone numbers, email addresses, or other PII outside the scope of operating the integration

5.5 Compliance Cooperation

- Provide tax forms, identity documentation, and beneficial ownership information as required
- Cooperate with INVO investigations into suspected fraud, abuse, or AUP violations
- Promptly notify INVO of any security incident affecting the Service, Player data, or Transactions
- Provide reasonable cooperation in connection with regulatory inquiries

6. Player-Specific Obligations

In addition to the general prohibitions in this AUP, Players agree to the following:

6.1 Account Use

- Use only one INVO account per person, unless INVO authorizes additional accounts
- Not share, sell, transfer, or rent your account or account credentials
- Maintain accurate account information, including current email and phone number
- Use account security features, including SMS verification and any additional security available

6.2 Payment Methods

- Use only payment methods you are authorized to use
- Not initiate chargebacks for Transactions you authorized and received the benefit of
- Resolve disputes with INVO support before contacting your bank or card issuer where reasonable

6.3 Virtual Currency Use

- Use Virtual Currency only within supported Games and authorized Service features
- Not attempt to convert Virtual Currency to cash outside authorized withdrawal mechanisms (where offered)
- Not buy, sell, or trade Virtual Currency or in-Game items outside the Service
- Not exploit bugs or glitches to generate Virtual Currency

6.4 Player Conduct

- Treat other Players, Developers, and INVO personnel with respect
- Not engage in harassment, threats, or abusive behavior
- Comply with the rules of any Game in which you participate
- Honor age requirements and obtain guardian consent if required

7. Enforcement

7.1 Investigation

INVO may investigate suspected violations of this AUP using methods INVO determines appropriate, including reviewing account activity, Transaction patterns, communications submitted through the Service, and information from third parties. INVO may request additional information or documentation from users in connection with investigations.

7.2 Available Actions

Where INVO determines that this AUP has been violated, or that a violation is reasonably suspected, INVO may take any one or more of the following actions, in INVO's sole discretion:

- Issue warnings, require corrective action, or impose enhanced monitoring
- Limit, restrict, or modify access to specific Service features
- Suspend the user's account, transactions, or payouts
- Terminate the user's account and access to the Service
- Reverse, hold, withhold, or claw back Transactions or balances
- Establish, increase, or extend reserves and hold periods
- Deduct amounts owed (including chargebacks, fees, and damages) from balances
- Refer the matter to law enforcement, regulators, banking partners, or industry consortiums
- Pursue all available legal remedies, including damages and injunctive relief
- Cooperate with platform providers, payment networks, or third parties to take consistent action

7.3 No Advance Notice Required

INVO is not required to provide advance notice before taking enforcement action, particularly in cases involving suspected fraud, security threats, regulatory compliance, harm to other users, or risk to the Service or its banking partners.

7.4 Severity-Based Response

INVO scales enforcement responses to the nature and severity of the violation. Minor or first-time violations may receive a warning or limited restriction; serious or repeated violations may result in immediate termination and legal action.

7.5 No Waiver

INVO's failure to enforce any provision of this AUP does not waive INVO's right to enforce it later. Selective enforcement does not create any precedent or commitment.

8. Reporting Violations

8.1 How to Report

If you become aware of conduct that violates this AUP, you may report it through the channels published in the INVO Policies. Reports should include: a description of the conduct, identifying information about the responsible user (if known), the dates and locations of the activity, and any supporting evidence.

8.2 Good Faith Reports

INVO will review reports submitted in good faith. Reports made in bad faith, with knowing falsity, or as part of harassment may themselves violate this AUP.

8.3 Confidentiality

INVO will treat the identity of reporters confidentially where reasonable, subject to legal obligations and the needs of investigation. INVO does not guarantee anonymity in all cases.

8.4 Mandatory Reporting

INVO reserves the right, and in some cases has the legal obligation, to report violations to law enforcement, regulators, or other authorities, including reporting child sexual abuse material to the National Center for Missing & Exploited Children (NCMEC) and other applicable bodies.

8.5 No Obligation to Investigate

INVO is not obligated to investigate every report and may prioritize investigations based on severity, evidence, and operational considerations.

9. Appeals

9.1 Right to Appeal

If your account or access to the Service has been suspended or terminated for a suspected AUP violation, you may submit an appeal through the channels published in the INVO Policies.

9.2 Appeal Process

Appeals must include: identifying account information, a description of the action being appealed, the basis for the appeal, and any supporting documentation. INVO will review appeals in good faith and respond within a commercially reasonable time.

9.3 Final Decisions

INVO's appeal decisions are final. INVO is not obligated to reverse enforcement actions even where the appellant believes the action was incorrect. Where applicable consumer protection law provides additional rights, those rights apply.

9.4 No Appeal for Severe Violations

INVO may decline to consider appeals for the most serious violations, including those involving illegal activity, child safety violations, severe fraud, security threats, or regulatory enforcement, except as required by applicable law.

10. General Provisions

10.1 Relationship to Other Documents

This AUP is part of the INVO Policies and is incorporated into the Developer Terms of Service and Player Terms of Service. In the event of a conflict between this AUP and the applicable Terms of Service, the Terms of Service control, except where this AUP provides more specific operational requirements consistent with the Terms.

10.2 Modifications

INVO may modify this AUP from time to time. Material changes are effective when posted, unless otherwise noted or required by applicable law. Continued use of the Service after modifications constitutes acceptance.

10.3 Severability

If any provision of this AUP is held unenforceable, the remaining provisions continue in full effect.

10.4 No Third-Party Beneficiaries

This AUP does not create any third-party beneficiary rights, except as expressly stated.

10.5 Examples Are Non-Exhaustive

The prohibited activities listed in this AUP are illustrative and not exhaustive. INVO may determine that conduct not specifically listed nonetheless violates the spirit and intent of this AUP.

10.6 Survival

Sections of this AUP that by their nature should survive termination of a user's account or access to the Service will do so, including without limitation provisions on enforcement, reporting, and general provisions.

--- END OF ACCEPTABLE USE POLICY ---