

PROHIBITED ITEMS & RESTRICTED ACTIVITIES POLICY

PREAMBLE

SellMMO Group FZ LLE, a company duly incorporated and validly existing under the laws of the Fujairah Creative City Free Zone, United Arab Emirates, acts solely as an Aggregator and Escrow Facilitator, and not as a direct seller of any in-game digital goods.

This Policy defines, for purposes of consumer transparency and lawful operation, the categories of items, services, and activities that are not permitted to be offered, displayed, marketed, transmitted, or otherwise facilitated through the Company's technical infrastructure.

It shall be construed *mutatis mutandis*, subject always to:

- (a) the applicable consumer-protection, e-commerce, data-protection, sanctions, and anti-fraud legislation of the European Union, the United Kingdom, the United States of America, and the United Arab Emirates;
- (b) the overarching principles of legality, proportionality, prudence, accountability, and fair-dealing; and
- (c) the Company's commitment to ensure that its Services remain compliant, safe, and consistent with lawful commercial conduct.

The Company acknowledges the importance of clearly identifying categories of goods, services, and digital items that are prohibited or restricted to protect Users, maintain platform integrity, and uphold its legal obligations.

Accordingly, this Policy is hereby adopted and published as the authoritative public statement of such prohibitions and restrictions applicable to all Buyers, Influencers, Sellers, and other Users engaging with SellMMO Group's Services, subject always to Applicable Law and without prejudice to the Company's legitimate interests.

SECTION 1 — DEFINITIONS

1.1. "Prohibited Item." For the purposes of this Policy, Prohibited Item shall mean, *mutatis mutandis* and without limitation, any good, service, digital asset, token, code, licence key, account, subscription, entitlement, access right, intangible benefit, or physical merchandise that is expressly banned, restricted, embargoed, proscribed, or otherwise excluded from lawful trade, sale, display, advertisement, escrow, facilitation, transmission, settlement, or fulfilment under (a) this Policy, (b) any other applicable public policy of the Company, or (c) Applicable Law.

This includes, *inter alia*, items contrary to intellectual-property rights, sanctions or export-control regimes, consumer-protection statutes, or publisher and end-user licence agreements.

For the avoidance of doubt, classification as a Prohibited Item may derive from the item's inherent characteristics, its provenance, its method of acquisition, or its reasonably foreseeable use.

1.2. "Restricted Activity." Restricted Activity shall mean any conduct, practice, omission, manipulation, circumvention, attempt, scheme, or transaction which, in the reasonable discretion

of the Company, poses or is likely to pose undue legal, regulatory, operational, reputational, technological, or financial risk to the Company, its partners, Buyers, or Influencers.

Such term shall include, *inter alia*, (a) any activity illustrated in Schedule A (Annexed List of Prohibited Items & Restricted Activities); (b) any conduct that undermines or frustrates the Company's lawful compliance and consumer-protection framework; and (c) any activity that a Competent Authority deems to constitute fraud, financial crime, unfair commercial practice, misrepresentation, or consumer detriment.

1.3. "Applicable Law." Applicable Law means all binding statutes, legislative instruments, regulations, ministerial decrees, circulars, interpretive notes, judicial precedents, or administrative practices issued by a Competent Authority that apply to a given transaction, activity, or person.

For the avoidance of doubt, this term expressly includes:

- (a) sanctions and export-control regimes administered by the United States (OFAC), the European Union, the United Kingdom, the UAE Central Bank, and the United Nations Security Council;
- (b) consumer-protection, data-protection, and e-commerce legislation, including the GDPR, UK GDPR, CPRA and comparable U.S. state-level privacy statutes, and the UAE PDPL; and
- (c) any successor enactments, amendments, or functionally equivalent norms, construed *mutatis mutandis*.

1.4. "Competent Authority." Competent Authority shall mean any governmental, regulatory, supervisory, judicial, arbitral, administrative, or enforcement body (*including, inter alia*, financial-intelligence units, data-protection authorities, consumer-protection agencies, gaming regulators, or international sanctions-enforcement bodies) having lawful jurisdiction over the Company, its Users, or its Services at any level. The term includes any successor or functionally equivalent body established under Applicable Law.

1.5. "User." User refers collectively and without limitation to all natural or legal persons interacting with the Company's Services, including Buyers, Influencers, Affiliates, Sellers (where such definition is not excluded by the Aggregator Role Disclaimer), and their authorised agents, representatives, or assigns.

1.6. "Services." Services shall mean the Company's websites, white-label storefronts, programmatic interfaces (APIs), escrow and settlement systems, and related functions—whether existing or later developed—through which transactions are initiated, routed, displayed, processed, or reconciled, subject always to the disclaimers and limitations set forth in this Policy and the Terms of Service (PP-1.1.1).

1.7. "Schedule A." For reference purposes only, Schedule A (Annexed List of Prohibited Items & Restricted Activities) refers to the internal and dynamic classification framework maintained by the Company to identify, review, and update categories of prohibited or restricted goods and activities. The Company may, from time to time, amend or expand such classifications in its discretion to reflect changes in Applicable Law or risk assessment.

The absence of any item or activity from publicly available descriptions shall not be construed as permission or waiver where the same falls within the broader scope of Clauses 1.1 or 1.2.

1.8. Interpretation. Unless the context requires otherwise: (a) singular includes plural and vice versa; (b) “including” or *inter alia* means “including without limitation”; (c) references to any law include amendments or successors; (d) headings are for convenience only and shall not affect interpretation; and (e) in the event of conflict, this Policy shall be interpreted consistently with the Terms of Service (PP-1.1.1) and Refund, Dispute & Buyer Protection Policy (PP-1.1.2).

1.9. “In-Game Valuables.” In-Game Valuables (also referred to as In-Game Assets) mean solely fungible in-game currencies or resources—such as coins, gold, crystals, credits, or comparable balance units—that exist exclusively within the environment of a multiplayer game or publisher platform and confer consumable or accumulative value strictly within that environment.

For clarity:

- (a) In-Game Valuables do not include accounts, characters, equipment, skins, cosmetic items, access keys, ancillary services, or any non-fungible tokens (NFTs) or crypto-assets;
- (b) the Company does not treat In-Game Valuables as securities, financial instruments, payment instruments, or virtual assets for regulatory purposes; and
- (c) all rights and obligations regarding In-Game Valuables are governed by the relevant Publisher End User Licence Agreement (EULA) and Applicable Law.

Nothing herein shall be construed as creating or transferring any real-world property or regulated financial asset through the facilitation of In-Game Valuables.

1.10. “Crypto Instruments.” Crypto Instruments refer to cryptocurrencies, stablecoins, digital tokens, or similar blockchain-based instruments; provided, however, that their acceptance or facilitation through the Company’s Services shall remain subject to the conditional limitations set forth in Section 3.3 of this Policy.

1.11. “Approved Crypto PSP.” Approved Crypto PSP means a duly licensed and authorised payment-service or virtual-asset-service provider that the Company has approved in writing to conduct crypto-settlement or custody services, subject to applicable regulatory requirements and contractual safeguards ensuring compliance, custodial insurance, and technical integration supporting secure escrow-based settlement.

SECTION 2 — SCOPE & APPLICABILITY

2.1 General Applicability

This Policy applies, mutatis mutandis, to all categories of Users, including Buyers, Influencers, Affiliates, Sellers, Fulfilment Partners and any other natural or legal persons who, whether directly or indirectly, intentionally or inadvertently, access, use, integrate with or otherwise benefit from the Company’s websites, white-label storefronts, Influencer storefronts, programmatic interfaces (APIs), escrow and reconciliation mechanisms, or any successor Services.

The term “User” shall be construed broadly and, subject always to Applicable Law, shall include authorised agents, representatives, employees, contractors and assigns acting on their behalf.

2.2 Commercial Focus and Product Scope — In-Game Valuables

This Policy has been formulated with the Company's principal commercial activity in mind — namely, the aggregation, facilitation and escrow-based settlement of transactions involving In-Game Valuables.

Such Valuables constitute the only permissible category of digital merchandise tradable through the Company's platforms, consistent with the Company's Terms of Service and Delivery and Fulfilment Policy.

Nothing herein shall be construed to create, assert or confer any off-platform property right, convertibility or legal characterisation of In-Game Valuables beyond the Publisher's ecosystem.

All Users remain bound by the relevant Publisher End User Licence Agreement (EULA) and Applicable Law.

2.3 Relationship to Other Policies

This Policy forms an integral component of the Company's Buyer-Facing Compliance Layer and shall be read in pari materia with the following instruments: Terms of Service; Refund, Dispute and Buyer Protection Policy; Delivery and Fulfilment Policy; Return and Warranty Policy; AML and CFT Policy; Sanctions and Fraud Compliance Statement; Privacy and Cookie Policy.

In the event of overlap or apparent inconsistency, the more specific or restrictive instrument shall prevail with respect to its subject matter, *mutatis mutandis*.

Where any provision of this Policy could reasonably be interpreted as more permissive than another policy, the stricter interpretation shall apply.

Buyer protections operate under the concept of an Acceptance Window, during which a Buyer may raise a dispute prior to escrow release, as defined in the Refund, Dispute and Buyer Protection Policy.

2.4 Territorial Reach

This Policy extends to all jurisdictions in which the Company's Services are lawfully accessible or targeted.

The application of this Policy across borders shall be interpreted in accordance with conflicts-of-law principles, mandatory local public policy and the overriding discretion of Competent Authorities.

2.5 Carve-Outs and Limitations

Notwithstanding anything to the contrary herein, this Policy does not apply to:

2.5.1 transactions or activities that are purely demonstrative, educational or otherwise non-executable within a commercial context;

2.5.2 activities expressly exempted under Applicable Law (narrowly construed); or

2.5.3 activities occurring exclusively on external peer-to-peer platforms not integrated with the Company's systems, except where the Company is legally or contractually required to exercise oversight.

2.6 Buyer Credentials and Fulfilment Exception

The Company recognises that, in limited circumstances, a Buyer may voluntarily provide temporary account credentials solely to enable order fulfilment (the “Fulfilment Exception”).

Such practice is permitted only under the following cumulative conditions:

2.6.1 Credentials must be submitted via the Company’s secure channel and used for a single, time-limited session.

2.6.2 Sellers, Influencers and Fulfilment Partners are strictly prohibited from storing, duplicating or retaining credentials beyond the immediate fulfilment window.

2.6.3 All credential use must be logged and auditable for dispute-resolution purposes, consistent with the Company’s internal data-protection framework.

2.6.4 Access must be limited to actions strictly necessary to complete delivery and must cease immediately upon confirmation of fulfilment.

2.6.5 Prior to transaction completion, Buyers must be presented with a clear risk disclosure acknowledging possible Publisher enforcement (e.g. account rollback or suspension) and the Company’s limited liability as set out in Section 6.

Any misuse or retention of credentials outside these parameters constitutes a material breach and shall be treated as a Restricted Activity subject to enforcement under Section 5.

2.7 Conditional Use of Crypto Instruments for Influencer Storefronts

Subject to Applicable Law, the Company may at its sole discretion permit the limited acceptance of Crypto Instruments as a means of payment through Influencer Storefronts, provided that the following conditions are continuously met:

2.7.1 Transactions must be processed solely through an Approved Crypto Payment Service Provider (PSP) holding all required licences or registrations and operating under Applicable Law.

2.7.2 Such PSP must apply robust AML / CFT controls, KYC and sanctions-screening procedures, and permit audit rights by the Company or Competent Authorities.

2.7.3 The Company shall not hold, convert or custody Crypto Instruments; settlement occurs exclusively within the Approved Crypto PSP’s infrastructure.

2.7.4 Buyers must receive clear pre-purchase disclosures about the volatility and regulatory risk of Crypto Instruments, their non-convertibility and the Company’s limited role.

2.7.5 The Company retains the right to suspend or disable Crypto payment options at any time for risk, regulatory or operational reasons.

2.7.6 Users remain solely responsible for any tax or reporting obligations arising from such payments.

Failure to satisfy these conditions renders the relevant Crypto payment option inactive and may trigger remedies under Section 5, including suspension and mandatory reporting.

2.8 Aggregator Role Disclaimer and Limits of Liability

Consistent with the Company’s Terms of Service, SellMMO Group acts solely as an Aggregator and technical facilitator.

It transmits orders, catalogue data and payment instructions between Buyers, Sellers, Influencers, Fulfilment Partners and third-party payment providers, but does not originate, own or control any In-Game Valuables.

Responsibility for the legality, authenticity and compliance of such items rests with the respective Sellers or Publishers, except as required by Applicable Law.

The Company's limited role is clearly disclosed in all storefront and transactional documentation.

2.9 Internal Classification Register (Informative Reference)

For transparency, the Company maintains an internal classification register identifying Prohibited Items and Restricted Activities.

This register is dynamic and subject to periodic review under the Company's compliance framework.

Its contents are not publicly disclosed, and absence of any item from public descriptions shall not be interpreted as permission or waiver where the conduct falls within the scope of this Policy or Applicable Law.

SECTION 3 — CATEGORIES OF PROHIBITED ITEMS

3.1 General Provisions

3.1.1 Without limitation, and subject always to periodic, version-controlled internal review under the Company's compliance framework, the following categories constitute Prohibited Items.

3.1.2 The lawful transfer of In-Game Valuables through temporary Buyer-provided credentials, where such transfer is necessary for the fulfilment of a bona fide order and executed strictly within the parameters set out in Section 2.6, shall not be deemed prohibited.

3.1.3 Any misuse, abuse or deviation from this narrowly permitted practice shall immediately convert the conduct into a Prohibited Item or Restricted Activity within the meaning of this Policy.

3.1.4 The Company maintains an internal classification register of Prohibited Items and Restricted Activities, which may be made available to Competent Authorities upon lawful request.

3.1.5 The lawful business of SellMMO Group FZ LLE extends exclusively to In-Game Valuables — virtual items such as gold, coins, crystals, credits or comparable digital currencies that exist solely within their respective game environments and have no independent real-world or wagering value.

3.1.6 The following activities shall not be authorised or tolerated:

3.1.6.1 engaging in gambling, betting, loot-box resale or any other form of game-of-chance monetisation;

3.1.6.2 issuing, exchanging or brokering cryptocurrencies, stablecoins or other crypto-assets requiring licence or registration under Applicable Law;

3.1.6.3 exchanging or “cashing out” In-Game Valuables for real-world money or crypto-assets outside the Company's authorised escrow and payment channels.

3.1.7 Any attempt to bypass approved settlement procedures or to privately negotiate peer-to-peer or off-platform payments is strictly prohibited and shall be treated as a Restricted Activity, potentially triggering suspension, escrow freeze or regulatory reporting under Sections 4 and 5.

3.2 Accounts and Credentials

3.2.1 Prohibited Conduct

3.2.1.1 The sale, resale, rental, transfer, listing or commercialisation of gaming accounts, login credentials or access rights that are stolen, hacked, compromised, misappropriated or shared across unrelated Buyers is prohibited.

3.2.1.2 The use or sale of accounts obtained in breach of contractual or legal restrictions applicable to such accounts (to the extent enforceable under Applicable Law) is prohibited.

3.2.1.3 The creation or distribution of synthetic, throw-away or fraudulent accounts intended to evade sanctions, platform restrictions or compliance controls is likewise prohibited.

3.2.2 Narrow Permitted Exception — Buyer Credentials for Fulfilment

3.2.2.1 The Fulfilment Exception defined in Section 2.6 applies exclusively to temporary, voluntary, Buyer-provided credentials.

3.2.2.2 All credential use must be logged and auditable strictly for dispute-resolution purposes, subject always to lawful data-retention requirements.

3.2.2.3 Disclosure of the Fulfilment Exception and any enforcement risk must be presented to the Buyer prior to payment within the escrow checkout flow.

3.2.2.4 Credentials must never be combined with payment instruments or crypto-settlement credentials governed by separate PSP requirements.

3.2.2.5 Any breach of these conditions shall reclassify the conduct as a Prohibited Item and trigger remedies under Section 5.

3.3 Automated Tools and Botting Services

3.3.1 Prohibited Conduct

3.3.1.1 Any script, bot, macro, exploit, automation routine or comparable software mechanism designed to interfere with, manipulate or gain unauthorised advantage within the Company's Services, escrow processes, storefront interfaces, API integrations or data flows is strictly prohibited.

This includes automated scraping, simulated transactions, bulk requests or any activity that distorts genuine user behaviour, system performance or transaction integrity.

Such prohibition applies regardless of intent or technical means and is enforced to preserve the stability, security and lawful operation of the Company's infrastructure.

3.3.1.2 The distribution, sale or provision of such tools — whether as software, hosting, subscription or service — is likewise prohibited.

3.3.2 Permitted Conduct (Narrow)

3.3.2.1 Manual fulfilment and lawful delivery actions performed by Sellers, Influencers or authorised Fulfilment Partners within the scope of the Company's approved fulfilment methods are permitted.

3.3.2.2 Any external automation used within third-party environments remains the sole responsibility of the respective User and shall not interface with, or affect, the Company's systems, escrow or compliance processes.

3.4 Digital Currencies and Tokens

3.4.1 Prohibited Conduct

3.4.1.1 The unlicensed sale, transfer, exchange, brokering or custody of cryptocurrencies, stablecoins, digital tokens or other Crypto Instruments without appropriate licences or exemptions under Applicable Law is prohibited.

3.4.1.2 Any structuring or disguising of fiat or crypto value as the sale of In-Game Valuables is likewise prohibited.

3.4.1.3 Where a digital instrument is deemed a regulated financial instrument under Applicable Law, facilitation thereof is prohibited unless expressly authorised.

3.4.2 Clarification re In-Game Valuables

3.4.2.1 In-Game Valuables (as defined in Clause 1.9) are not Digital Currencies or Crypto Instruments by virtue of existing solely within their respective game environments.

3.4.2.2 Legitimate in-game currency delivered through lawful digital-delivery mechanisms under the Company's escrow arrangements shall not be treated as a Digital Currency.

3.4.2.3 Any attempt to disguise fiat or crypto transactions as in-game currency delivery constitutes regulatory circumvention and shall be reported to Competent Authorities.

3.5 Real-World Currencies and Payment Instruments

3.5.1 Unlicensed fiat exchanges, money-remittance services, prepaid or stored-value instruments (including stolen or cloned cards) and resale-restricted or region-locked gift cards or vouchers obtained in breach of scheme rules or law are prohibited.

3.6 High-Risk Goods and Services

3.6.1 The following categories are prohibited without exception:

3.6.1.1 gambling, wagering, betting, sweepstakes or lottery services;

3.6.1.2 adult or sexually explicit services;

3.6.1.3 narcotics, controlled substances, precursors or drug paraphernalia;

3.6.1.4 weapons, ammunition, explosives, fireworks or hazardous materials;

3.6.1.5 malware, spyware, hacking kits, phishing infrastructure or other cyber-offensive tools.

3.7 Intellectual Property and Digital Integrity

3.7.1 Any counterfeit, pirated, unauthorised or otherwise infringing digital goods, activation keys, serials, licences or works that violate applicable intellectual-property law are strictly prohibited.

3.7.2 The Company prohibits the listing or resale of digital items or assets that originate from exploitation of software vulnerabilities, duplication methods or other unintended technical behaviours of external systems or games, where such conduct would reasonably compromise lawful ownership or the integrity of transactions within the Company's Services.

3.8 Sanctioned Goods or Services

3.8.1 Transactions involving sanctioned persons, entities or jurisdictions are prohibited, including indirect routings intended to evade sanctions.

3.8.2 All Users must comply with the Company's sanctions-screening and due-diligence requirements.

3.9 Misuse of Buyer Credentials

3.9.1 The following conduct is expressly prohibited:

3.9.1.1 retaining Buyer-provided credentials after the fulfilment session;

3.9.1.2 accessing unrelated accounts, inventories or content using Buyer credentials;

3.9.1.3 duplicating, copying, selling, transferring to any third party or storing Buyer credentials beyond the permitted fulfilment window;

3.9.1.4 creating, marketing or offering "credential-based services" for hire.

3.9.2 Any violation of this Clause constitutes a Restricted Activity and may result in suspension, escrow clawback and reporting to Competent Authorities.

3.10 Prohibited Tangible Goods

3.10.1 Physical merchandise that is illegal, counterfeit, unsafe or otherwise contrary to consumer-protection or export-control law (including recalled or banned products) is prohibited when offered through the Company's Services.

3.10.2 Sellers remain responsible for ensuring product safety, authenticity and lawful sourcing.

3.11 Protection of Minors

3.11.1 Any listing, service, communication, advertisement or delivery mechanism that targets, solicits or is likely to be accessed or purchased by persons under eighteen (18) years of age is strictly prohibited.

3.11.2 The Company does not knowingly permit the sale or delivery of In-Game Valuables to minors.

3.11.3 Attempts to circumvent age restrictions by misrepresenting age or identity constitute a Restricted Activity enforceable under Section 5.

3.11.4 The Company shall comply with all applicable child-protection laws, including the GDPR (Article 8), UK GDPR, COPPA and UAE PDPL, and may require age verification or parental consent to ensure compliance.

SECTION 4 — RESTRICTED ACTIVITIES

The following practices, being inconsistent with the principles of legality, prudence, proportionality and transparency, constitute Restricted Activities.

Such conduct is subject to enforcement under Sections 5 and 6 and may, depending on gravity, also amount to a Prohibited Item under Section 3 or under Applicable Law.

The list below is illustrative and non-exhaustive; the Company retains exclusive and reasonable discretion to determine, ex aequo et bono, whether any behaviour falls within this category, subject always to its monitoring, investigatory and remedial powers.

4.1 Circumvention Schemes

4.1.1 Any attempt, device or stratagem intended, designed or reasonably likely to bypass, frustrate or impair the Company's Payment and Escrow Infrastructure shall constitute circumvention.

4.1.2 Restricted practices include, *inter alia*:

- 4.1.2.1 inducing, encouraging or assisting any User to transact off-platform to evade commissions, escrow protections or compliance screening;
- 4.1.2.2 using alternative or unapproved payment rails, merchant descriptors or routing paths;
- 4.1.2.3 fragmenting, structuring or disguising transactions to evade reporting thresholds, sanctions filters or AML/Fraud controls;
- 4.1.2.4 tampering with Storefront or API code to disable escrow, traceability or fee capture mechanisms.

4.1.3 Authorised penetration testing or technical audit shall be lawful only under a Company-initiated or mutually executed written engagement specifying scope, confidentiality and indemnity obligations.

4.1.4 Any breach hereof may result in immediate suspension, escrow freeze and regulatory notification.

4.2 Misrepresentation

4.2.1 The making of any false, misleading or incomplete statement, omission or representation concerning provenance, ownership, authenticity, rarity, legality or quality of In-Game Valuables, accounts or services is prohibited.

4.2.2 Illustrative cases include:

- 4.2.2.1 exaggerating scarcity or uniqueness without verifiable substantiation;
- 4.2.2.2 representing used or re-sold items as new, exclusive or publisher-issued;
- 4.2.2.3 concealing material reliance on third-party Fulfilment Partners or publisher constraints;
- 4.2.2.4 omitting information a reasonable Buyer would require to make an informed choice.

4.2.3 Minor catalogue reproductions of official publisher text shall not, *per se*, constitute misrepresentation if accurately quoted.

4.2.4 Persistent or material misrepresentation may be treated as a fraudulent act under Section 5, triggering restitution and indemnity obligations.

4.3 Artificial Scarcity, Bundling and Urgency Mechanics

4.3.1 It is prohibited to fabricate or simulate scarcity, limited availability or urgency with intent to manipulate Buyer perception or decision-making.

4.3.2 Examples include:

- 4.3.2.1 creating unauthorised "exclusive packs", deceptive countdowns or false limited edition labels;
- 4.3.2.2 deploying pseudo-scarcity UX or algorithmic throttling to mislead Buyers;
- 4.3.2.3 using visual indicators implying stock depletion without verifiable basis.

4.3.3 Buyer-approved bundles or combinations explicitly requested by Buyers remain lawful, provided all representations are accurate, transparent, and do not mislead or misrepresent the scope, content, or value of the offered In-Game Valuables.

4.3.4 Violation of this Clause may result in de-listing, monetary penalties and Seller reputation downgrade.

4.4 Credential Misuse Beyond Delivery

4.4.1 Beyond the narrowly-defined Fulfilment Exception (see Section 2.6), the following practices are restricted:

4.4.1.1 retaining, copying, archiving or storing Buyer credentials beyond the fulfilment session;

4.4.1.2 accessing unrelated game areas, inventories or communications;

4.4.1.3 using Buyer credentials for analytics, profiling, marketing or any secondary commercial purpose;

4.4.1.4 selling, transferring or re-using Buyer credentials to create credential-based services.

4.4.2 Each instance of credential misuse constitutes a material breach and may trigger immediate account suspension, escrow forfeiture and mandatory regulatory reporting.

4.5 Manipulation of Escrow, Dispute and Resolution Mechanisms

4.5.1 Manipulative or abusive engagement with escrow, dispute or rating systems is strictly prohibited.

4.5.2 Illustrative forms include:

4.5.2.1 collusive or sham disputes intended to obtain unjust refunds;

4.5.2.2 submission of falsified or misleading evidence or screenshots;

4.5.2.3 deliberately exploiting timing windows to induce automatic escrow release;

4.5.2.4 filing repetitive or vexatious disputes to harass counterparties.

4.5.3 Confirmed abuse shall lead to dispute-handling privilege revocation, escrow clawback, and potential referral to payment networks or authorities.

4.6 Exploitative Marketing, Targeting and Promotion

4.6.1 All Users engaging in promotion, advertising or content publication shall adhere to responsible-marketing principles.

4.6.2 Prohibited conduct includes:

4.6.2.1 making unsubstantiated or deceptive claims of performance, rarity or advantage;

4.6.2.2 employing coercive or predatory upselling or cross-selling tactics;

4.6.2.3 targeting minors or vulnerable individuals with age-inappropriate content or incentives;

4.6.2.4 failing to disclose paid sponsorships, influencer remuneration or affiliate links;

4.6.2.5 using prohibited imagery, hate symbols or language contrary to publisher standards.

4.6.3 Compliant influencer disclosures that are transparent, auditable and in good faith shall not be deemed exploitative.

4.6.4 The Company may suspend or remove marketing assets, impose disclosure templates or require remedial training for repeat offences.

4.7 Data, Privacy and Security Violations

4.7.1 The protection of personal data and digital integrity forms a core compliance obligation.

4.7.2 Restricted behaviour includes:

4.7.2.1 harvesting, scraping or storing Buyer data beyond legitimate fulfilment or audit needs;

4.7.2.2 selling, leasing or disclosing personal data to unauthorised parties;

4.7.2.3 profiling, cross-platform tracking or re-identification without lawful basis;

4.7.2.4 failure to honour Buyer data-subject rights or maintain appropriate technical and organisational safeguards.

4.7.3 Violations shall be addressed in accordance with Applicable Law and may result in data-handling suspension, mandatory re-certification or regulatory disclosure.

4.7.4 Where a breach endangers consumer rights or system integrity, the Company reserves the right to enact immediate containment and coordinate with competent data-protection authorities.

4.8 Collusion, Market Manipulation and Anti-Competitive Conduct

4.8.1 All forms of collusion or coordinated market distortion are forbidden.

4.8.2 Examples include:

4.8.2.1 coordinated false orders, phantom trades or wash transactions to inflate metrics;

4.8.2.2 price-fixing, reciprocal discounting or pre-arranged trading circles;

4.8.2.3 collective exclusion or blacklisting designed to impair competitor access or manipulate visibility rankings.

4.8.3 Such conduct may violate competition law and shall be reported to regulators where legally required.

4.8.4 The Company may apply algorithmic audits, ranking penalties or account deactivation to restore market integrity.

4.9 Abuse of Platform Integrity and Security Controls

4.9.1 Conduct undermining the reliability or orderly operation of the Company's ecosystem is prohibited.

4.9.2 This includes:

4.9.2.1 mass-posting or duplicate-listing spam designed to distort catalogue search;

4.9.2.2 reverse-engineering APIs, exploiting vulnerabilities or injecting unauthorised code to gain advantage;

4.9.2.3 interfering with compliance, audit or forensic monitoring.

4.9.3 Any security testing, vulnerability assessment, or research activity involving the Company's systems, APIs, or infrastructure is strictly prohibited unless expressly initiated, commissioned, or authorised in writing by the Company itself under a defined and pre-approved scope, confidentiality undertaking, and indemnity conditions.

4.9.4 Unauthorised interference may lead to permanent account termination and, where applicable, referral for criminal investigation.

4.10 Inducement of Off-Platform Transactions and Fee Evasion

4.10.1 It is prohibited to solicit, persuade or encourage Buyers, Sellers or Influencers to transact, negotiate or settle outside the Platform.

4.10.2 Restricted acts include:

4.10.2.1 sharing personal contact or payment details to bypass escrow;

4.10.2.2 offering direct-deal discounts or conditional incentives tied to off-platform settlement;

4.10.2.3 migrating catalogues or customer relationships to unmonitored systems to evade oversight.

4.10.3 Such behaviour compromises consumer protection and financial-crime safeguards and will result in fee forfeiture, listing removal and account restriction.

4.11 Fraudulent, Abusive or Synthetic Behaviour

4.11.1 Any scheme or device involving deception, identity manipulation or transactional falsification is restricted.

4.11.2 Illustrative forms include:

4.11.2.1 multi-account or referral fraud networks;

4.11.2.2 velocity or timing manipulation to evade monitoring triggers;

4.11.2.3 social-engineering, SIM-swap or credential-stuffing techniques;

4.11.2.4 chargeback abuse or friendly fraud aimed at unjust enrichment.

4.11.3 The Company shall employ automated fraud-detection analytics, pattern correlation and manual reviews.

4.11.4 Confirmed fraudulent conduct may lead to permanent termination, asset forfeiture and reporting to Competent Authorities.

4.12 Regulatory Escalation and Reporting

4.12.1 Any conduct reasonably suspected to involve money-laundering, terrorist financing, sanctions evasion, fraud or other criminality shall be subject to immediate escalation, temporary suspension and forensic evidence preservation.

4.12.2 The Company may, to the extent required or expressly permitted by Applicable Law, submit suspicious-activity or incident reports to Competent Authorities within jurisdictions having lawful supervisory or enforcement competence, and always in accordance with its internal AML/CFT escalation procedures and data-protection obligations.

4.12.3 While the Company shall exercise discretion to prevent frivolous reporting, it shall not be fettered in fulfilling statutory reporting duties or lawful requests for assistance.

4.12.4 Users are expected to cooperate fully with any resulting investigation and to preserve relevant records or correspondence when requested.

SECTION 5 — ENFORCEMENT & REMEDIES

5.1 General Enforcement Authority

5.1.1 The Company shall at all times reserve, retain and may exercise, in its sole, reasonable and unfettered discretion, all corrective, interim, provisional and final measures necessary to safeguard the integrity, security and orderly functioning of its Services.

5.1.2 Such measures may be exercised without prior notice or justification, save where notice is required by Applicable Law or by the Company's internal due-process framework.

5.1.3 The Company may act immediately where urgency, suspected fraud, systemic abuse or regulatory risk is reasonably perceived; provided however that, where practicable and not precluded by law or exigent circumstances, affected Users shall be afforded an opportunity to respond once enforcement has been implemented.

5.1.4 The Company's enforcement powers shall be construed mutatis mutandis with its contractual, statutory and fiduciary duties to Buyers, Influencers, Affiliates and third-party partners.

5.2 Illustrative Measures

5.2.1 Without limitation to the general authority under Clause 5.1, the Company's enforcement measures may include, *inter alia*:

5.2.1.1 Suspension or Termination — suspending, disabling, restricting or permanently terminating User access, accounts, credentials or API keys, whether wholly or in respect of specific Storefronts.

5.2.1.2 Content and Catalogue Actions — removing, disabling, re-labelling or de-listing any offer, listing, catalogue entry, promotional content or Storefront found inconsistent with this Policy or Applicable Law.

5.2.1.3 Escrow and Asset Control — withholding, freezing, quarantining, clawing back, redirecting or re-escrowing funds, In-Game Valuables or other assets held under the Company's control pending the outcome of internal investigations, dispute resolution or regulatory requests.

5.2.1.4 Crypto-Specific Safeguards — for transactions involving Crypto Instruments, imposing additional safeguards including:

5.2.1.4.1 temporary quarantines or technical holds on crypto funds;

5.2.1.4.2 mandatory conversion or routing through an Approved Crypto PSP;

5.2.1.4.3 reversal or tracing where technically and contractually feasible;

5.2.1.4.4 refusal to accept non-approved on-chain transfers for escrowed transactions; provided however that irreversible on-chain transfers initiated outside an Approved Crypto PSP flow may not be recoverable and shall not, absent gross negligence or wilful misconduct by the Company, give rise to Company liability.

5.2.1.5 Regulatory and Third-Party Reporting — escalating or notifying suspected violations, offences or irregularities to any Competent Authority, Payment Service Provider, Approved Crypto PSP, or other legally entitled third party, together with supporting records or forensic summaries

strictly limited to what is required or expressly permitted by Applicable Law and the Company's data-protection framework.

For the avoidance of doubt, the Company shall not disclose transactional, user, or forensic data to Publishers, External Platforms, or other non-regulatory parties unless compelled by lawful process or necessary to protect the Company's own legal rights and interests.

5.2.1.6 Civil and Equitable Remedies — pursuing civil, contractual or statutory relief, including specific performance, restitution, indemnification, injunctive relief (including ex parte emergency orders), damages, accounts of profits and recovery of costs and interest before competent courts or arbitral tribunals.

5.2.1.7 Administrative and Remediation Measures — imposing transaction limits, temporary or permanent credential re-verification, enhanced due diligence, remediation plans, appointment of supervised monitors, or heightened behavioural oversight.

5.2.1.8 Forensic Preservation — ordering preservation, capture and retention of data, logs, communications and other evidence (including mirror images of wallets or accounts) for a reasonable period, and sharing such materials with Competent Authorities subject to lawful process.

5.2.1.9 Financial Remedies — imposing fees, penalties, restitution or set-off against escrow balances to recoup losses, remediation costs (including forensic and provider expenses), and legal fees reasonably incurred by the Company.

5.3 Interim and Emergency Relief

5.3.1 Where there is a reasonable basis to suspect imminent loss, fraud, sanctions evasion or other systemic abuse (including credential misappropriation or diversion of funds), the Company may implement immediate interim measures such as:

5.3.1.1 emergency suspension of affected accounts;

5.3.1.2 temporary holds on funds or assets;

5.3.1.3 urgent co-operation with Approved Crypto PSPs or PSPs to preserve assets or evidence.

5.3.2 Such measures may be taken without prior judicial or arbitral process; provided however that the Company shall adopt proportionate responses and, where practicable, document reasons and notify affected Users post-factum.

5.4 Proportionality, Risk-Based Application and Escalation

5.4.1 All enforcement shall be applied on a risk-sensitive and proportionate basis, taking into account:

5.4.1.1 the gravity and materiality of the breach;

5.4.1.2 potential or actual harm to Buyers, Influencers or third parties;

5.4.1.3 the User's compliance history and responsiveness;

5.4.1.4 the availability and credibility of evidence; and

5.4.1.5 the Company's regulatory and contractual duties.

5.4.2 Where acute risk exists (e.g., suspected sanctions breach or large-scale fraud), the Company may prioritise immediate containment over graduated escalation without waiving subsequent rights to apply further remedies.

5.5 Cumulative Remedies and No Waiver

5.5.1 The remedies set forth herein are cumulative and non-exclusive and may be exercised concurrently or sequentially.

5.5.2 No exercise, omission or delay in exercising any remedy shall constitute a waiver of any future right or enforcement action.

5.5.3 The Company expressly reserves all rights and remedies not expressly limited or excluded hereby, subject always to Applicable Law.

5.6 Co-operation with Competent Authorities and Third Parties

5.6.1 The Company shall co-operate, to the extent required or expressly permitted by Applicable Law, with Competent Authorities, Payment Service Providers, Approved Crypto PSPs, and other legally entitled third parties in relation to lawful investigations, regulatory inquiries, or remedial actions.

For the avoidance of doubt, such co-operation shall not extend to Publishers, External Platforms, or other non-regulatory entities, unless the Company is compelled by lawful process or acts to protect its own legal rights, compliance position, or financial interests.

5.6.2 Such co-operation shall be conducted in accordance with Applicable Law and the Company's confidentiality and data-protection framework.

5.6.3 Where disclosure of sensitive information is required, the Company shall seek appropriate protective mechanisms (including mutual legal assistance channels or confidentiality orders) to safeguard commercial and personal data

5.7 Allocation of Costs, Indemnification and Remedies for Breach

5.7.1 Any User determined, after due investigation, to have materially breached this Policy shall indemnify and hold harmless the Company, its Affiliates, Subsidiaries and respective officers, directors, employees and agents from and against all losses, liabilities, damages, costs and expenses (including reasonable legal fees and forensic costs) incurred as a result of such breach.

5.7.2 The Company may, to the extent permitted by law, deduct or set off such amounts from funds held in escrow or otherwise payable to the User.

5.7.3 Nothing in this Clause shall preclude the Company from seeking additional statutory or equitable relief as may be available under Applicable Law.

5.8 Notice and Dispute Procedure

5.8.1 Where the Company initiates or implements any enforcement measure, it shall, where lawful and practicable, notify the affected User through its designated communication channels in accordance with the Internal Guidelines on Contract Administration and User Agreement Management.

5.8.2 Users may contest any enforcement decision exclusively through the Company's internal dispute-resolution mechanism and, where applicable, before competent judicial or arbitral fora as provided in the relevant Terms of Service.

5.8.3 All interim, precautionary, or emergency measures shall remain fully effective and enforceable pending final determination, unless and until revoked by the Company or a competent judicial or arbitral authority.

5.8.4 The Company shall record, archive, and retain copies of all enforcement communications, correspondence, and related notices as part of its Compliance Evidence & Audit Pack, for transparency, traceability, and evidentiary purposes.

5.9 Record-Keeping and Retention

5.9.1 The Company shall maintain complete and verifiable records of investigations, enforcement actions, dispute files, forensic materials, and related evidence for not less than the minimum period required by Applicable Law, or for such longer period as prescribed under its internal Document Retention Schedule.

5.9.2 Evidentiary copies may be preserved beyond the standard retention period where reasonably necessary for ongoing investigations, regulatory co-operation, audit readiness, or the defence and assertion of the Company's legal rights and interests.

5.9.3 All records shall be created, stored, accessed, and destroyed in accordance with the Data & Information Security Policy and the Internal Data Protection and DSAR Response Procedure, ensuring confidentiality, integrity, and non-repudiation throughout their lifecycle.

SECTION 6 — DISCLAIMER

6.1 Aggregator Role

6.1.1 The Company acts solely and exclusively as an Aggregator and technical facilitator within the meaning of this Policy.

6.1.2 The Company's functions are strictly limited to transmitting, routing, mirroring, indexing and recording catalogues, orders, payment instructions, fulfilment requests and associated metadata between Buyers, Sellers, Influencers, Affiliates, Payment Service Providers ("PSPs"), Approved Crypto PSPs and Fulfilment Partners.

6.1.3 Except where expressly agreed in writing, the Company does not originate, manufacture, own, control, store, warranty, or assume any proprietary or custodial interest in any In-Game Valuables, digital goods, accounts, credentials or physical merchandise offered through its Services.

6.1.4 The facilitation role of the Company shall be construed narrowly, solely for the purpose of enabling order routing, escrow settlement and compliance oversight, and shall not be interpreted as:

6.1.4.1 a transfer or conveyance of ownership or title to any item;

6.1.4.2 an endorsement, certification or assurance of authenticity; or

6.1.4.3 a guarantee of merchantability, fitness, legality or publisher compliance.

6.1.5 For the avoidance of doubt, all In-Game Valuables exist solely within the virtual environments and data architectures of respective Publisher Platforms.

While such items may possess contractual or transactional value as between Users under this Policy, they do not constitute legal tender, securities, or independently recognised financial instruments under Applicable Law.

Nothing in this Clause shall be construed as a concession of ownership, intellectual-property, or proprietary rights to any Publisher, nor as an acknowledgment that In-Game Valuables are devoid of lawful or assignable value within the scope of the Company's Aggregator Services.

6.2 Absence of Publisher Control and No Publisher Warranty

6.2.1 The Company has no editorial, operational or enforcement authority over any Publisher, Publisher Platform or game developer.

6.2.2 The Company shall not be responsible for any enforcement, restriction, rollback, suspension, reversal, deletion, or other remedial action undertaken by a Publisher or platform operator.

6.2.3 Buyers and Sellers acknowledge that Publisher actions may include loss of items, bans, or rollbacks beyond the Company's control.

6.2.4 Provided however that the Company may, at its sole discretion and without prejudice to its independence, issue non-binding informational notices or general risk advisories to Users, or engage in limited, good-faith technical coordination with external game operators solely for the purpose of mitigating widespread service disruptions or systemic compliance risks; such coordination shall not create any agency, partnership, endorsement, or obligation toward any Publisher, nor shall it be interpreted as recognition of any Publisher's authority or rules as binding upon the Company.

6.2.5 No part of this Policy shall be interpreted as creating a warranty or assurance that any transaction or item will be accepted, maintained or recognised by any Publisher.

6.3 Allocation of Obligations and Buyer Assumption of Risk

6.3.1 All obligations, representations, warranties and covenants regarding the legality, authenticity, fitness, availability, or publisher-compliance of any In-Game Valuables rest exclusively with the Seller, Influencer or Fulfilment Partner, as applicable.

6.3.2 Prior to completing any transaction, each Buyer represents and warrants that:

6.3.2.1 they are legally competent to contract and not a minor under the applicable age of majority;
6.3.2.2 they understand that In-Game Valuables exist only within a Publisher Platform, cannot be redeemed for fiat currency, and possess no guaranteed real-world value;

6.3.2.3 they have read and accepted both the Publisher's EULA and the Company's pre-purchase disclosures, including all risk caveats.

6.3.3 Buyers further acknowledge that the regulatory classification of virtual goods may vary across jurisdictions and that the Company does not guarantee the legal status, tradability, or marketability of any such item.

6.3.4 The Company shall not be liable for misunderstandings, misrepresentations or losses arising from differing national interpretations of “digital goods”, “virtual property” or “in-game currency” unless caused by the Company’s gross negligence or wilful misconduct.

6.4 Limitation of Liability

6.4.1 To the fullest extent permitted by Applicable Law, and subject to mandatory consumer-protection provisions, the Company disclaims all liability (direct, indirect, incidental, consequential or exemplary) arising out of or relating to:

6.4.1.1 the acts or omissions of Sellers, Influencers or Fulfilment Partners;

6.4.1.2 the legality, authenticity, quality or continued functionality of any In-Game Valuables or Publisher goods;

6.4.1.3 account suspensions, revocations or rollbacks imposed by Publishers;

6.4.1.4 freezes, holds or reversals imposed by PSPs, acquiring banks, card schemes or Approved Crypto PSPs;

6.4.1.5 misaddressed on-chain transfers, private key compromise or other crypto-specific loss outside the Company’s custody;

6.4.1.6 system outages, maintenance, force majeure or events beyond reasonable control.

6.4.2 Notwithstanding the foregoing, nothing herein shall exclude liability which cannot be waived under Applicable Law, including liability for gross negligence, wilful misconduct or fraudulent misrepresentation by the Company.

6.4.3 The Company’s aggregate liability toward any User shall, in any event, be limited to the lesser of: (i) the amount of the relevant transaction held in escrow, or (ii) one hundred United States dollars (USD 100), unless a higher amount is required by Applicable Law.

6.5 Data Protection, Privacy and Statutory Compliance

6.5.1. The Company’s handling of personal data shall comply with applicable data-protection legislation, including without limitation the EU General Data Protection Regulation (EU GDPR), the UK General Data Protection Regulation (UK GDPR), the United Arab Emirates Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL), and the California Privacy Rights Act (CPRA), insofar as each is applicable to the User and to the processing activity in question.

6.5.2. The Company processes User data solely for legitimate purposes directly connected with the operation of the Platform, including order routing, escrow management, fraud prevention, dispute handling, risk and sanctions screening, and regulatory or supervisory compliance, as further described in the Company’s publicly published Privacy & Cookie Policy (including Exhibit 1 – Cookie Notice), which is hereby incorporated by reference for data-protection purposes.

6.5.3. Nothing in this Policy shall derogate from or limit the mandatory rights of data subjects/User-consumers under applicable data-protection legislation, including the rights of access, rectification, erasure, restriction, objection, portability, and the right to lodge a complaint with a competent Data Protection Authority.

6.5.4. The Company shall cooperate with competent Data Protection Authorities and shall maintain appropriate technical and organisational safeguards in accordance with its Data &

Information Security Policy. Where the Company has appointed, or is required to appoint, an EU or UK data-protection representative, the contact details of such representative(s) shall be set out in the Company's Privacy & Cookie Policy and shall serve as the primary point of contact for EU/UK data subjects and supervisory authorities in those territories.

6.5.5. Users acknowledge that the Company may disclose personal or transactional data solely to Payment Service Providers, sanctions/AML screening providers, or competent regulatory, supervisory or law-enforcement authorities, and only where such disclosure is strictly necessary for statutory compliance, fraud prevention, or lawful enforcement under Applicable Law.

6.5.6. For the avoidance of doubt, the Company shall not disclose or transmit any User data to Publishers, game operators, or other non-regulatory third parties unless compelled by lawful process (such as a court order, warrant, or regulatory directive) or where such disclosure is strictly necessary to protect the Company's own legal rights or to prevent imminent harm to the User, the Platform, or other Users. Any such disclosure shall remain subject to the Company's Data & Information Security Policy and applicable data-protection legislation.

6.6 Publisher Enforcement Caveat and Allocation of Risk

6.6.1 The Company bears no responsibility or liability for any enforcement, penalty, rollback or restriction imposed by a Publisher resulting from ordinary or foreseeable fulfilment methods, including:

6.6.1.1 temporary use of Buyer credentials for fulfilment (the Fulfilment Exception);

6.6.1.2 in-game mail or auction-house transfers;

6.6.1.3 marketplace trading or overlay interfaces;

6.6.1.4 anti-cheat, fraud or detection systems.

6.6.2 Buyers acknowledge that these fulfilment methods may trigger Publisher responses or enforcement outside the Company's control.

6.6.3 The Company shall not, under any circumstances, be responsible or liable for any enforcement, penalty, restriction, rollback, suspension, confiscation, or other action taken by a Publisher or platform operator that arises from the Buyer's own in-game behaviour, account activity, or rule violations.

To the extent permitted by Applicable Law, a Buyer who voluntarily provides account credentials for fulfilment acknowledges and accepts full responsibility for any consequences arising within the Publisher's environment, including account restrictions or enforcement measures, without recourse against the Company.

The Company's responsibility is strictly limited to the integrity of its own escrow, payment, and delivery systems, and it shall not be deemed to supervise, control, or guarantee any Buyer's or Seller's conduct inside any external game or platform.

Nothing in this Clause shall, however, exclude the Company's liability in cases of its own gross negligence or wilful misconduct.

6.6.4 The Company shall not rely on this disclaimer to exclude liability in cases of its own proven gross negligence or deliberate misconduct.

6.7 Crypto and Irreversibility Caveat

6.7.1 Where crypto-asset payments are enabled, the Company's role shall be strictly limited to technical facilitation of settlement through an Approved Crypto PSP.

The Company does not itself hold, store, convert, exchange, broker, intermediate, or otherwise exercise possession or control over any crypto-assets or private keys at any stage of the transaction.

All custody, conversion, and on-chain processing are executed exclusively by the relevant Approved Crypto PSP under its own licence, regulatory supervision, and contractual framework.

For the avoidance of doubt, the Company shall not be deemed a virtual-asset service provider ("VASP"), custodian, money transmitter, or financial intermediary under any Applicable Law, and bears no liability for on-chain execution, gas fees, or blockchain network performance, save where loss is directly caused by the Company's gross negligence or wilful misconduct.

6.7.2 The Company does not itself hold, exchange, convert or manage crypto assets unless expressly authorised by contract.

6.7.3 Users acknowledge and accept that:

6.7.3.1 blockchain transactions are irreversible once broadcast;

6.7.3.2 mis-addressed transfers or private-key losses are technically unrecoverable;

6.7.3.3 crypto payments are governed by the relevant Approved Crypto PSP's own terms and conditions.

6.7.4 The Company shall not be liable for any crypto-related loss or delay except where arising from the Company's gross negligence, wilful misconduct or breach of its written obligations toward an Approved Crypto PSP.

6.7.5 All Users are responsible for understanding local tax, accounting and reporting duties related to crypto transactions.

6.8 No Endorsement and No Guarantee of Legality

6.8.1 The Company does not endorse, sponsor, or warrant the legality or compliance of any In-Game Valuables, listings, Sellers, Influencers or Fulfilment Partners in any jurisdiction.

6.8.2 Listings and integrations appearing on the Platform are provided "as-is", subject to Seller responsibility and Applicable Law.

6.8.3 The Company expressly disclaims any guarantee that use of its Services will be lawful, permissible or risk-free in every jurisdiction or under every Publisher rule.

6.8.4 Each User is solely responsible for ensuring that their activities on or through the Company's Services comply with Applicable Law, including but not limited to consumer-protection, data-protection, sanctions, export-control and anti-fraud regulations in their jurisdiction.

For the avoidance of doubt, compliance with any Publisher's internal rules, community standards or end-user licence terms remains the independent responsibility of the User vis-à-vis that Publisher and does not form part of the Company's contractual or regulatory obligations.

The Company neither enforces nor interprets Publisher policies and shall not be deemed to guarantee their observance.

6.9 Buyer Acknowledgement and Pre-Purchase Consent

6.9.1 Before completing any transaction involving account-credential access, crypto settlement, or high-value in-game delivery, the Buyer shall be required to acknowledge and accept the associated risks via an explicit, affirmative confirmation (e.g., checkbox, signature, or digital timestamp).

6.9.2 This acknowledgement constitutes binding evidence that the Buyer has:

6.9.2.1 read and understood this Section 6;

6.9.2.2 accepted the specific risks of Publisher enforcement, account suspension and crypto irreversibility; and

6.9.2.3 consented to the Company's limited aggregator role and absence of direct liability.

6.9.3 Transactions without such explicit acknowledgement shall not proceed, and the Company may cancel, freeze or reject them without liability.

6.10 Survival, Severability and Interpretation

6.10.1 The provisions of this Section 6 shall survive termination, expiry or suspension of this Policy to the extent necessary to preserve their protective effect.

6.10.2 If any provision herein is found invalid or unenforceable in any jurisdiction, such invalidity shall not affect the remaining provisions, which shall continue in full force to the maximum extent permitted by law.

6.10.3 Headings are for convenience only and shall not affect interpretation.

6.10.4 This Section 6 shall be construed harmoniously with the Terms of Service, Refund & Buyer Protection Policy, Privacy & Cookie Policy and other incorporated instruments, each reinforcing the Company's limited facilitation role.

SECTION 7 — ENTIRE AGREEMENT & GOVERNING LAW

7.1 Integration and Entire Agreement

7.1.1 This Policy, together with the Company's Terms of Service, Refund & Buyer Protection Policy, Privacy & Cookie Policy, and all other Public Policies expressly incorporated by reference, constitutes the entire agreement between the Buyer and the Company in relation to the subject matter hereof.

7.1.2 All prior statements, representations, promotional materials or communications (not expressly incorporated in writing and signed by an authorised representative of the Company) shall be deemed non-binding and shall not give rise to any contractual rights or obligations.

7.1.3 This Clause does not derogate from any non-waivable consumer protection rights mandated under Applicable Law.

7.2 Hierarchy and Interpretation

7.2.1 In the event of any conflict or inconsistency between this Policy and another Incorporated Policy of the Company, the following hierarchy shall apply in descending order of precedence:

(a) mandatory provisions of Applicable Law;

(b) the more specific or restrictive Company Policy governing the particular subject matter;

(c) this Policy; and

(d) any general ancillary terms or guidelines.

7.2.2 Where ambiguity arises, the Company shall interpret provisions in good faith and in a manner that advances compliance, prudential protection, consumer safety and the public interest, mutatis mutandis.

7.3 Governing Law

7.3.1 This Policy shall be governed by and construed in accordance with the laws of the United Arab Emirates (UAE), and specifically the laws and regulatory framework of the Fujairah Creative City Free Zone, without regard to conflicts-of-law principles.

7.3.2 For the avoidance of doubt, nothing in this Clause shall exclude the application of mandatory consumer-protection, data-protection, e-commerce or financial-compliance laws in other jurisdictions where such laws apply by virtue of their extraterritorial reach or public-policy status.

7.3.3 Should any jurisdiction's law require the application of its own mandatory provisions (for example, consumer rights in the EU, UK or US), such provisions shall prevail only to the extent they cannot lawfully be contracted out of.

7.4 Jurisdiction and Dispute Resolution

7.4.1 Primary Jurisdiction

Except as otherwise stipulated below and save where prohibited by Applicable Law, the competent courts of the Emirate of Fujairah (UAE) shall have non-exclusive jurisdiction to hear and determine any dispute, controversy or claim arising out of or relating to this Policy.

7.4.2 Interim Relief

Either party may apply to any competent court for urgent interim injunctive, preservatory or conservatory relief (including ex parte orders) to protect confidential information, intellectual property or assets, or to prevent irreparable harm. Such application shall not constitute a waiver of arbitration rights where applicable.

7.4.3 Arbitration Option

(a) The Company may, at its sole discretion and at the time of instituting proceedings, elect to refer any dispute (excluding applications for urgent interim relief) to binding arbitration administered by one of the following institutions:

- (i) the DIFC-LCIA Arbitration Centre (Dubai International Financial Centre);
- (ii) the London Court of International Arbitration (LCIA); or
- (iii) the International Chamber of Commerce (ICC).

(b) The seat and procedural law of arbitration shall be determined in accordance with the chosen institution's rules and the Company's election; provided however that the Company may select a seat within the UAE or any internationally recognised neutral venue.

(c) The language of arbitration shall be English. The Company may require an expedited procedure where circumstances so justify.

7.4.4 Waiver of Multiplicity

To the fullest extent permitted by law, parties agree that they shall not pursue duplicative proceedings in multiple fora in respect of the same claim, and that the Company's election of arbitration under Clause 7.4.3 shall be final and binding.

7.4.5 Enforcement of Awards

Any arbitral award shall be final and binding on the parties and may be entered and enforced in any court of competent jurisdiction pursuant to the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 1958).

7.5 Language and Authentic Version

7.5.1 This Policy has been drafted and executed in the English language. The English text shall be the sole authoritative version for purposes of interpretation and enforcement.

7.5.2 Translations provided in other languages are for convenience only; in the event of conflict or ambiguity, the English version shall prevail to the fullest extent permitted by law.

7.6 Severability and Survival

7.6.1 If any provision of this Policy is held to be invalid, illegal or unenforceable by a court or tribunal of competent jurisdiction, the remaining provisions shall remain in full force and effect.

7.6.2 The parties shall endeavour in good faith to replace any invalid clause with a valid one that most closely reflects the original commercial intent and risk allocation.

7.6.3 All provisions which, by their nature or intent, are intended to survive termination (including without limitation those relating to liability limitations, arbitration, governing law and confidentiality) shall so survive and remain enforceable mutatis mutandis.

SCHEDULE A — ANNEXED LIST OF PROHIBITED ITEMS & RESTRICTED ACTIVITIES (Public Version)

Preamble

For the avoidance of doubt, this Schedule forms an integral part of the Prohibited Items & Restricted Activities Policy and shall be read mutatis mutandis with all other public policies of SellMMO Group FZ LLE.

Its purpose is to define, in a transparent and non-exhaustive manner, the principal categories of items, practices and activities that are prohibited or restricted within the Company's Services, Storefronts, and affiliated environments, in order to preserve integrity, legality, and consumer protection.

Absence of a specific item or activity from this Schedule shall not be construed as permission or waiver where such conduct falls within the broader meaning of Clauses 1.1 or 1.2 of the main Policy.

1. Accounts & Access Data

1.1 Any sale, resale, transfer, rental, or exchange of user accounts, access data, or credentials obtained through unauthorised, deceptive, or unlawful means is strictly prohibited.

1.2 Retention or reuse of Buyer-provided credentials after the completion of fulfilment, duplication or storage of access tokens, or any unauthorised use of account data constitutes a restricted activity.

1.3 The Company prohibits the creation or distribution of synthetic, throwaway or fraudulent accounts, including those intended to evade enforcement, manipulate in-game economies, or mislead other users.

1.4 Sellers and Influencers may not store or copy Buyer credentials outside the secure session used for fulfilment.

1.5 The Company reserves the right to monitor, suspend or report any credential-related activity that threatens security or consumer trust.

2. Automation & Bots

2.1 The use, provision or facilitation of bots, scripts, macros, cheat engines, automation services, or similar tools that interfere with the normal operation of the Company's platform, storefronts or fulfilment systems is prohibited.

2.2 Automated access, data scraping, denial-of-service attempts or mass interactions with the Company's infrastructure are expressly forbidden.

2.3 Automation or scripting applied within third-party environments remains the sole responsibility of their publishers and users; however, such automation must never connect, interact with, or affect the Company's systems, APIs, or escrow environment.

2.4 The Company may block, suspend, or technically limit automated activity to protect its operations, infrastructure integrity, and service availability.

2.5 This Clause does not restrict lawful, internal automation performed by the Company itself for risk management, compliance screening, or performance optimisation purposes.

3. Currencies & Value Transfers

- 3.1 Unauthorised sale, exchange, or facilitation of cryptocurrencies, tokens, stablecoins or any digital representations of value outside the Company's approved payment channels is prohibited.
- 3.2 Users shall not disguise or mislabel currency or crypto transactions as "in-game valuable" transfers for the purpose of avoiding regulation, escrow control or payment supervision.
- 3.3 Where permitted, digital currency payments must flow exclusively through Company-approved payment service providers and in accordance with the relevant terms.
- 3.4 The Company may suspend, delay, or refuse any transaction that raises compliance, sanctions or money-laundering concerns.
- 3.5 Any attempt to exchange, hedge, or net-settle outside authorised PSPs shall constitute a material breach and may trigger permanent suspension and reporting to competent authorities.

4. High-Risk Goods & Activities

- 4.1 The following categories are absolutely prohibited and shall not be listed, promoted or transacted through the Company's services:
 - 4.1.1 Gambling, wagering or lottery services of any form;
 - 4.1.2 Adult or sexually explicit material or services;
 - 4.1.3 Controlled substances, narcotics or related paraphernalia;
 - 4.1.4 Weapons, explosives or dual-use items;
 - 4.1.5 Malicious software, hacking tools or penetration-for-hire services;
 - 4.1.6 Any other goods or services which the Company reasonably deems to present legal, regulatory, safety or reputational risk.
- 4.2 Any attempt to conceal or disguise such activity will be treated as a material breach and may result in permanent suspension and reporting to competent authorities.

5. Fraud, Misrepresentation & Deceptive Practices

- 5.1 False, misleading, or deceptive representations concerning the origin, authenticity, ownership or legality of any in-game item, service or listing are strictly prohibited.
- 5.2 The use of fabricated evidence, falsified screenshots, or simulated trades to induce a sale constitutes a fraudulent activity.
- 5.3 Any attempt to manipulate escrow, dispute, or refund systems by collusion, shill activity or "friendly fraud" will result in immediate enforcement under Section 5 of the main Policy.
- 5.4 Sellers, Influencers and Affiliates must represent their offers transparently, and Buyers are expected to act in good faith during any transaction or dispute.

6. Sanctions & Restricted Jurisdictions

- 6.1 Transactions involving sanctioned persons, entities or jurisdictions are prohibited.
- 6.2 Users must not attempt to route or disguise payments, assets or accounts in order to bypass international sanctions or regulatory restrictions.

6.3 The Company conducts screening against relevant sanctions lists and may freeze, hold or refuse funds or transactions where sanctions exposure is detected.

6.4 The authoritative list of restricted jurisdictions shall be maintained and periodically published by the Company.

7. Credential Use & Security

7.1 Credentials provided by Buyers may be used only for the narrow and time-limited purpose of order fulfilment under the Company's supervision.

7.2 Sellers and Influencers must not store, duplicate or transmit such credentials beyond the fulfilment window.

7.3 Any use of credentials to access unrelated data, accounts or inventories is prohibited.

7.4 The Company may implement secure-channel delivery, monitoring and deletion procedures to ensure confidentiality and to detect misuse.

8. Market Integrity & Fair Conduct

8.1 False or misleading descriptions, fabricated scarcity claims, collusive pricing, or manipulative trading intended to distort market perception are prohibited.

8.2 Review fraud, shill listings, wash trades or circular transactions are likewise prohibited.

8.3 Influencers and Sellers must disclose sponsored promotions or affiliate relationships.

8.4 The Company reserves the right to adjust or remove any listing or content found to manipulate the marketplace or mislead Buyers.

9. Escrow & Dispute Integrity

9.1 Fraudulent or collusive disputes, fabricated evidence or coordinated chargebacks constitute restricted activities.

9.2 The Company may withhold, re-escrow or reverse payments where dispute abuse is suspected.

9.3 All Users must act in good faith during dispute resolution and provide truthful, verifiable information.

9.4 Repeated or serious abuse of escrow or chargeback mechanisms may result in permanent suspension and reporting to payment partners or authorities.

10. Off-Platform Dealings

10.1 Users may not solicit or induce others to complete payments or transfers outside the Company's escrow or approved payment channels.

10.2 Any listing, message or content inviting "direct deals", external wallet transfers or private settlements constitutes off-platform solicitation.

10.3 The Company may suspend or delist Users who attempt to divert transactions off-platform.

10.4 Permissible community or non-commercial communication remains allowed, provided no external payment or inducement is offered.

11. Data Protection & Privacy

11.1 Unauthorised harvesting, retention, or sharing of Buyer personal data is prohibited.

11.2 Data may be processed only to the extent necessary for lawful fulfilment, escrow, or compliance purposes.

11.3 Onward sale, marketing use or profiling based on Buyer data without explicit consent is forbidden.

11.4 The Company maintains privacy-by-design safeguards and reserves the right to enforce immediate suspension or deletion for data-handling breaches.

Closing Provision

This Schedule shall be deemed incorporated into and form an integral part of the Prohibited Items & Restricted Activities Policy of SellMMO Group FZ LLE.

In the event of inconsistency, the stricter provision shall prevail, mutatis mutandis.

Publication of this Schedule on the Company's official portal constitutes sufficient notice to all Users.