ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING (AML & CFT) STATEMENT

PREAMBLE

This Anti-Money Laundering and Counter-Terrorist Financing Statement (hereinafter, the "Policy") forms an integral component of SellMMO Group's Buyer-Facing Compliance Layer and establishes the principles by which SellMMO Group FZ LLE, a company duly incorporated and validly existing under the laws of the Fujairah Creative City Free Zone, United Arab Emirates (hereinafter, the "Company"), ensures that its platform, escrow systems, and payment processes are not misused for purposes of Money Laundering, Terrorist Financing, or other illicit activities.

The Company acts solely as an Aggregator and Escrow Facilitator, providing technical, operational, and compliance infrastructure to enable lawful peer-to-peer exchanges of in-game digital valuables. It does not act as a direct seller of such assets.

This Policy shall be interpreted *mutatis mutandis* and in accordance with:

1. Federal Law No. 20 of 2018 on Anti-Money Laundering and Countering the Financing of Terrorism and Illegal Organisations of the United Arab Emirates, together with Cabinet Decision No. 10 of 2019 and subsequent implementing regulations;
2. The recommendations and interpretive notes of the Financial Action Task Force (FATF), including the risk-based approach (Recommendation 1), customer due diligence (Recommendation 10), record-keeping (Recommendation 11), suspicious-transaction reporting (Recommendation 20), and transparency of beneficial ownership (Recommendation 24);
3. The equivalent anti-money-laundering and counter-terrorist-financing obligations under the laws of the European Union, the United Kingdom, and the United States of America, to the extent applicable; and
4. The Company's overarching commitment to responsible business conduct, proportionality, and transparency within the meaning of international compliance standards.

For avoidance of doubt, internal operating manuals and technical procedures referenced in the Company's internal documentation (including those concerning audit cadence, transaction screening, and internal data handling) are not part of this public statement but are applied in accordance with the Company's internal information-security and compliance framework, ensuring the confidentiality, integrity, and lawful processing of all information.

The Company acknowledges the growing regulatory emphasis on Virtual Asset Service Providers (VASPs) under frameworks such as UAE VARA, the EU Markets in Crypto-Assets Regulation (MiCA), and comparable international regimes. Accordingly, where virtual-asset payments are processed, the Company applies risk-based and proportionate controls consistent with applicable FATF standards.

By this Policy, the Company reaffirms its commitment to:

- Prevent its services from being exploited for Money Laundering or Terrorist Financing;

- Uphold transparency of beneficial ownership across its influencer, affiliate, and partner networks; and
- Maintain, review, and continually enhance its AML/CFT framework to remain aligned with evolving legal and regulatory obligations.

SECTION 1 — DEFINITIONS

For the purposes of this Anti-Money Laundering and Counter-Terrorist Financing Statement, and unless the context otherwise requires, the following terms shall have the meanings assigned to them hereunder.

1.1 “Money Laundering” means any act or attempted act intended to conceal, disguise, convert, transfer, or otherwise legitimise the proceeds of crime, including by way of placement, layering, or integration into the lawful economy, contrary to Applicable Law.

1.2 “Terrorist Financing” means the provision, collection, transfer, or management of funds or other assets, by any means, directly or indirectly, with the intention that they be used, or with the knowledge that they are to be used, in whole or in part, to support or carry out terrorist acts or benefit terrorist organisations.

1.3 “Beneficial Owner” means the natural person or persons who ultimately own or control a customer, or on whose behalf a transaction is conducted, including those who exercise ultimate effective control over a legal person or arrangement, consistent with Financial Action Task Force (FATF) Recommendation 24 and other Applicable Law.

1.4 “Know-Your-Customer” or “KYC” means the identification and verification procedures applied by the Company to confirm the identity of Users, partners, or other counterparties before or during the course of a business relationship.

1.5 “Politically Exposed Person” or “PEP” means any individual who is or has been entrusted with a prominent public function, together with their immediate family members and known close associates, as defined by Applicable Law and relevant FATF guidance.

1.6 “Suspicious Transaction Report” or “STR” means a formal report submitted to the competent authority where there are reasonable grounds to suspect that funds are the proceeds of crime or are related to Terrorist Financing, in accordance with Applicable Law.

1.7 “User” or “Customer” means any natural or legal person who accesses, registers for, or transacts through the Company’s platform or affiliated storefronts, whether as Buyer, Seller, Influencer, or Fulfilment Partner, as further defined in the Company’s Terms of Service (PP-1.1.1).

1.8 “Customer Due Diligence” or “CDD” means the baseline identification, verification, and risk-assessment measures applied to Users in accordance with FATF Recommendation 10.

“Enhanced Due Diligence” or “EDD” means the application of additional or more intrusive measures in higher-risk situations, such as dealings with PEPs, complex structures, cross-border transactions, or transactions involving virtual assets.

1.9 “Risk-Based Approach” or “RBA” means the proportional methodology by which the Company applies controls commensurate with the level of risk identified, consistent with FATF Recommendation 1 and prevailing international standards.

1.10 “Virtual Asset” means a digital representation of value that may be digitally traded, transferred, or used for payment or investment purposes, excluding digital representations of fiat currency.

“Virtual Asset Service Provider” or “VASP” means any entity engaged in one or more of the activities described in FATF Recommendation 15 or its local implementing regulations, including exchange, transfer, safekeeping, administration, or other services related to Virtual Assets.

1.11 “Sanctioned Person” means any individual or entity designated under sanctions lists issued by the United Nations, European Union, United Kingdom, United States, United Arab Emirates, or any other competent authority.

“Restricted Jurisdiction” means any country or territory subject to comprehensive trade or financial sanctions, embargoes, or equivalent restrictions under Applicable Law.

1.12 “Red Flags” or “Risk Indicators” means patterns, behaviours, transaction types, or other characteristics that may reasonably be considered indicative of potential Money Laundering, Terrorist Financing, sanctions evasion, or other illicit conduct, as recognised in FATF guidance and regulatory advisories.

SECTION 2 — SCOPE & APPLICABILITY

2.1 Users and Jurisdictions.

This Policy applies to all Users, including Buyers, Influencers, Affiliates, and any other natural or legal persons using the Company’s services, to the extent and within those jurisdictions where SellMMO Group FZ LLE qualifies as, or is treated as, a reporting entity under Applicable Law.

For the avoidance of doubt, external Sellers who transact exclusively through independent peer-to-peer (P2P) marketplaces are not directly onboarded by the Company. Responsibility for their customer identification and verification (KYC/Customer Due Diligence) rests with the relevant P2P provider. The Company acts solely in its capacity as an Aggregator and Escrow Facilitator, not as a direct seller of in-game valuables.

Nevertheless, where such transactions pass through the Company’s escrow, payment, or technical infrastructure, the Company applies proportionate monitoring and sanctions-screening controls consistent with its overall compliance and anti-fraud framework, ensuring that all flows are lawfully processed and free from misuse.

2.2 Covered Transactions.

This Policy encompasses all transactions processed, routed, or escrowed by the Company, including without limitation:

- payment initiation and settlement;
- refund or chargeback handling;
- dispute resolution and buyer-protection workflows; and
- temporary risk holds or compliance-related transaction delays.

All such activities are conducted subject to Applicable Law and in accordance with the Company’s broader contractual and compliance obligations.

For clarity, crypto-asset payments and settlements are considered Covered Transactions whenever the Company acts as, or is deemed to be, a Virtual Asset Service Provider (VASP) within the meaning of FATF Recommendation 15 or comparable regulatory standards. The Company applies a risk-based and proportionate approach to such activities, ensuring alignment with prevailing global AML/CFT expectations.

2.3 Institutional Counterparties.
The Company may maintain business relationships with institutional counterparties such as external P2P platforms, payment-service providers, or settlement intermediaries. In such cases, the Company conducts Know-Your-Business (KYB) verification proportionate to risk and limited to:

- confirmation of corporate identity and registration;
- screening against sanctions and adverse-media lists;
- identification of beneficial ownership (where feasible and proportionate); and
- verification of relevant regulatory or licensing status.

These counterparties remain independently responsible for their own user-level compliance obligations. The Company performs ongoing oversight of institutional partners commensurate with their assessed risk exposure, applying a Risk-Based Approach (RBA) consistent with FATF Recommendation 1 and Applicable Law.

SECTION 3 — CUSTOMER DUE DILIGENCE (CDD / KYC)

3.1 Standard Due Diligence.
The Company applies identification and verification procedures consistent with Applicable Law and international AML/CFT standards.

For each category of User — including Influencers, Affiliates, and other parties receiving remuneration — the Company collects the minimal information necessary to verify identity and legitimacy. Verification may rely on government-issued identification, electronic or biometric verification systems (where legally permissible), and other authoritative databases or public registers.

For Buyers, the Company applies a simplified due-diligence approach unless specific risk indicators or enhanced due-diligence triggers are present.

Where permitted by law, the Company may rely on verification already performed by regulated third parties (such as licensed payment-service providers or financial institutions). However, such reliance does not exempt the Company from maintaining its own risk-based monitoring and fraud-detection controls.

For avoidance of doubt, external Sellers transacting exclusively via independent P2P platforms are not directly onboarded by the Company. Responsibility for their KYC/CDD lies with the respective P2P provider. The Company's role is confined to that of an Aggregator and Escrow Facilitator, ensuring that technical and transactional channels remain compliant and secure.

Standard CDD measures are designed to ensure compliance with the Company's broader risk management, sanctions screening, and prohibited-activities controls, as referenced across other

public policies — notably the Prohibited Items & Restricted Activities Policy (PP-1.2.1) and the Refund, Dispute & Buyer Protection Policy (PP-1.1.2) — as well as to maintain proper documentation and auditability.

3.2 Enhanced Due Diligence (EDD).

The Company applies enhanced verification and monitoring in situations where higher risks of Money Laundering or Terrorist Financing are identified. Such circumstances may include, without limitation:

- dealings with Politically Exposed Persons (PEPs) or their close associates;
- cross-border transfers involving high-risk or sanctioned jurisdictions;
- complex or unusually large transactions lacking clear economic rationale;
- virtual-asset payments or settlements; or
- opaque ownership structures suggesting elevated risk.

Enhanced Due Diligence may include verification of source of funds and source of wealth, senior management approval prior to establishing or continuing a relationship, and closer monitoring of transaction behaviour throughout the engagement.

All such measures are applied on a risk-proportionate basis, consistent with FATF Recommendation 10, FATF Recommendation 24, and applicable national AML/CFT regulations.

3.3 Ongoing Due Diligence and Monitoring.

The Company maintains both periodic reviews and continuous monitoring of customer information and transactional activity to ensure records remain current and relevant. Monitoring includes the use of automated tools to identify unusual activity, behavioural anomalies, or “red-flag” patterns indicative of layering, sanctions evasion, or other suspicious conduct.

Where new information arises or risk profiles change, the Company updates records and re-validates identity as required by law.

All personal and transactional data obtained or generated under this Section are retained and safeguarded in accordance with Applicable Law and the Company’s internal data-protection and retention framework, ensuring confidentiality, integrity, and lawful processing.

SECTION 4 — TRANSACTION MONITORING

4.1 Ongoing Monitoring.

The Company conducts continuous and proportionate monitoring of all transactions processed through its escrow, settlement, and payment systems to identify potential indicators of Money Laundering or Terrorist Financing. Monitoring is performed on a risk-based basis, with the scope, frequency, and depth of review determined by the User’s risk profile, transaction type, and jurisdictional exposure.

4.2 Analytical and Screening Controls.

To ensure effective oversight, the Company employs a combination of technical and procedural controls that may include, inter alia:

- threshold- and velocity-based triggers;

- behavioural or pattern-recognition analytics;
- automated sanctions-list screening;
- virtual-asset tracing and blockchain-analysis tools (where applicable); and
- geographic or jurisdictional risk indicators designed to identify unusual, inconsistent, or suspicious transactional behaviour.

These measures are applied in accordance with the principles of FATF Recommendation 20 and Applicable Law, ensuring that suspicious activity is identified promptly and reviewed by authorised personnel.

4.3 Suspension and Escalation of Transactions.
Where a transaction or activity raises suspicion of illicit conduct, the Company may, without prior notice, delay, suspend, or block such transaction pending internal review.

If suspicion is substantiated, the Company shall:

- escalate the matter to its appointed Compliance Officer / Money Laundering Reporting Officer (MLRO);
- submit a Suspicious Transaction Report (STR) to the competent authority in accordance with Applicable Law; and
- take proportionate remedial actions, which may include account suspension, escrow reversal, or termination of access to the Services.

All such actions are undertaken in accordance with legal obligations and the Company's broader compliance framework, always subject to the principles of fairness, proportionality, and confidentiality.

4.4 Documentation and Record Retention.
All alerts, escalations, investigations, and compliance actions undertaken under this Section are formally documented and securely retained for the period required by law.

Records are maintained in a manner ensuring integrity, auditability, and confidentiality, consistent with the Company's internal information-security and data-protection standards.

SECTION 5 — REPORTING OBLIGATIONS

5.1 Suspicious Activity and Transaction Reports (SAR / STR).
Where required by Applicable Law, the Company files Suspicious Activity or Suspicious Transaction Reports (collectively, "STRs") with the competent Financial Intelligence Unit in the relevant jurisdiction.

All employees, contractors, and authorised partners are obliged to promptly escalate any suspicion of Money Laundering, Terrorist Financing, sanctions evasion, or other financial crime to the Company's appointed Compliance Officer / Money Laundering Reporting Officer (MLRO).

The MLRO evaluates each escalation and determines whether a report must be submitted to the competent authority. Such filings are made within the statutory deadlines and in accordance with the procedural requirements of the jurisdiction concerned.

5.2 Cooperation with Authorities.
The Company cooperates fully with regulatory, supervisory, and law-enforcement authorities in any legitimate investigation relating to the prevention or detection of Money Laundering or Terrorist Financing, subject always to Applicable Law, data-protection requirements, and confidentiality obligations.

Where a transaction involves multiple jurisdictions, the Company coordinates its obligations to ensure that reports are filed timely, accurately, and to the appropriate competent authority.

5.3 Prohibition on Tipping Off.
In strict compliance with law, the Company and its personnel must not disclose to any User, counterparty, or unauthorised person that a suspicious-activity report has been or may be filed.

All internal reporting and subsequent handling of suspicions are conducted strictly on a need-to-know basis, ensuring confidentiality and integrity of any regulatory communication.

5.4 Record Keeping.
The Company maintains secure, confidential, and tamper-resistant records of:

- internal escalations and reviews;
- decisions and justifications of the MLRO;
- submitted STRs and corresponding acknowledgements; and
- any related regulatory correspondence.

Such records are retained for the period required by Applicable Law, ensuring their authenticity, integrity, and accessibility to competent authorities upon lawful request. Data retention is carried out in line with the Company's internal information-security and data-protection framework, consistent with the principles of lawfulness, purpose limitation, and proportionality.

5.5 Whistleblower Protection.
Any employee, contractor, or partner who, in good faith, reports or escalates a suspicion of Money Laundering, Terrorist Financing, or other financial misconduct shall not be subject to retaliation, dismissal, or adverse treatment for having made such a report.

This protection is afforded in line with Applicable Law and international best practices, reinforcing the Company's commitment to a culture of integrity, transparency, and compliance.

SECTION 6 — RECORD KEEPING

6.1 Retention Period.
The Company retains all documentation and records relevant to its anti-money-laundering and counter-terrorist-financing obligations — including but not limited to KYC, Customer Due Diligence (CDD/EDD), transaction data, monitoring results, internal reviews, and any related compliance reports — for a minimum of five (5) years from the later of:

(i) the completion of the transaction, or

(ii) the termination of the business relationship.

Longer retention may apply where required by Applicable Law or by instruction of a competent authority.

All retention activities are subject to the principles of data-minimisation, purpose limitation, and proportionality, ensuring that data are preserved only to the extent necessary for legal, regulatory, or evidentiary purposes.

6.2 Security and Accessibility of Records.
All records are stored and maintained in a manner that ensures their authenticity, integrity, and tamper-evidence.

Records must be readily retrievable upon lawful request by competent authorities and protected through appropriate technical and organisational safeguards.

Access to such data is strictly limited to authorised personnel on a need-to-know basis and is logged to maintain auditability and accountability.

6.3 Cross-Border Data Compliance and Review.
Where any portion of the Company's records is stored, processed, or mirrored across multiple jurisdictions, such storage is governed by the relevant cross-border-data-transfer laws, including but not limited to the EU GDPR, UK GDPR, and UAE Personal Data Protection Law (PDPL).

The Company periodically reviews its retention and deletion practices to ensure they remain appropriate, proportionate, and compliant with evolving international and national regulatory requirements.

SECTION 7 — TRAINING & AWARENESS

7.1 Training Obligations.
The Company shall provide structured and role-specific Anti-Money-Laundering and Counter-Terrorist-Financing (AML/CFT) training to all relevant employees, managers, officers and contractors whose duties involve, directly or indirectly, customer interaction, transaction processing, compliance oversight or technical support. Such training shall be delivered upon commencement of engagement and at regular intervals thereafter, but in any event not less than once per calendar year, and shall be proportionate to the individual's responsibilities and risk exposure.

7.2 Training Content.
The scope of AML/CFT training shall, at a minimum, encompass the identification and recognition of suspicious activities and red-flag indicators; the proper internal procedures for escalation and reporting; the legal and regulatory duties imposed under Applicable Law; awareness of sanctions-compliance requirements; the lawful handling of virtual-asset transactions; and the principles of data protection and confidentiality as they relate to the prevention of financial crime. All content shall be designed to ensure that personnel are capable of detecting, reporting and mitigating the risks of Money Laundering and Terrorist Financing in practice.

7.3 Delivery and Methodology.
Training shall be conducted through an appropriate combination of delivery methods consistent with the Company's compliance framework, including, inter alia, interactive sessions, remote or e-

learning modules, and knowledge-validation exercises. The chosen methodology shall ensure effective comprehension, retention and application of the material by participants.

7.4 Training Records.
The Company shall maintain accurate and verifiable records of all AML/CFT training conducted, including the identity of participants, the content delivered, and the results of any assessments or evaluations. Such records shall be preserved for the period prescribed by Applicable Law and shall remain available for inspection by competent authorities, ensuring transparency and accountability.

7.5 Continuous Review and Improvement.
The content of AML/CFT training shall be reviewed at least annually and, where necessary, updated more frequently to reflect emerging risks, changes in legislation or regulation, technological developments, and lessons derived from audits, supervisory feedback or enforcement actions. The Company shall thereby ensure that all relevant personnel remain adequately informed, competent and vigilant in the ongoing prevention of Money Laundering and Terrorist Financing.

SECTION 8 — GOVERNANCE & AUDIT

8.1 Compliance Governance.
The Company shall designate a duly qualified Compliance Officer / Money Laundering Reporting Officer (MLRO) who shall bear ultimate responsibility for the design, implementation and ongoing oversight of the Company's Anti-Money-Laundering and Counter-Terrorist-Financing (AML / CFT) framework. The MLRO shall have sufficient authority, independence, and access to information and resources to discharge their duties effectively and shall report directly to the General Manager, who acts as the ultimate AML-responsible person in accordance with the Central Bank of the UAE Guidance for Licensed Financial Institutions on AML / CFT (Circular No. 2021 / 01). The MLRO shall be responsible for the escalation of compliance and risk issues to senior management, the review and handling of internal reports under Section 5, and the maintenance of communication and liaison with regulators, supervisory bodies and other competent authorities, ensuring that all regulatory notifications and requests for information are addressed promptly, accurately and in compliance with Applicable Law. For the avoidance of doubt, the MLRO shall operate with full autonomy within the scope of their mandate, subject always to the oversight of the General Manager and the governance principles established under the Company's internal compliance and audit framework.

8.2 Business-Wide Risk Assessment and Internal Audit.
The Company shall undertake a documented Business-Wide Risk Assessment (BWRA) and shall conduct periodic internal audits at intervals proportionate to its overall risk exposure, but in any event not less than once annually. Additional assessments shall be performed whenever material changes occur in the Company's business model, product suite, technological infrastructure or risk profile, including (but not limited to) the introduction of virtual-asset or crypto-denominated payments. The Company may, at its discretion, engage independent external auditors to validate the effectiveness and proportionality of its AML / CFT controls.

8.3 Scope of Audit and Assessment.
The scope of the BWRA and related audit activities shall encompass, inter alia, customer onboarding and due-diligence procedures (CDD / EDD), transaction monitoring, sanctions screening, suspicious-transaction reporting processes, training and awareness programmes, and record-keeping compliance. All audit methodologies shall ensure evidentiary sufficiency, proportionality and independence in accordance with internationally recognised standards and best practice.

8.4 Reporting and Remediation.
Findings of each BWRA and audit shall be formally reported to the General Manager and, where relevant, to the MLRO. The Company shall implement appropriate corrective and remedial actions in a timely manner, and shall maintain documented evidence of remediation, follow-up testing and closure of all identified issues to demonstrate continuous improvement and regulatory accountability.

8.5 Retention and Confidentiality.
All BWRA documents, audit reports, remediation plans and related records shall be securely retained in accordance with Section 6 (Record Keeping) and the Company's internal information-security and data-protection framework. Such records shall be preserved in a manner that ensures their authenticity, integrity and availability for lawful inspection by competent authorities, subject always to Applicable Law and the Company's legitimate interests.

ANNEXES (Public Reference Overview)

A. Risk-Based Approach Statement — The Company maintains an internal framework governing risk identification and mitigation, aligned with FATF Recommendation 1.

B. KYC & Verification Procedures — The Company applies proportionate verification standards consistent with Applicable Law; procedural details are maintained internally.

C. Suspicious Activity Reporting Standards — The Company utilises a confidential template and secure reporting channels for STR filings with competent authorities.

All annexes referenced above are maintained as controlled internal documents and are made available to regulatory or supervisory bodies upon lawful request.