SANCTIONS & FRAUD COMPLIANCE STATEMENT

1. PREAMBLE

1.1 This Sanctions & Fraud Compliance Statement (hereinafter, the "Policy") is adopted and publicly issued by SellMMO Group FZ LLE, a juridical person duly incorporated and validly existing under the laws of the Fujairah Creative City Free Zone, United Arab Emirates (License No. 14608/2019, P.O. Box 4422, UAE), acting at all times in its capacity as an Aggregator and technical facilitator, rather than as a direct seller or merchant of record of digital goods or in-game valuables. This Policy shall be interpreted mutatis mutandis and shall be interpreted in accordance with the Company's applicable compliance and security standards, including its anti-money-laundering, data-protection, and internal-control frameworks as updated from time to time.

1.2 This Policy reflects the Company's adherence to the applicable sanctions, export-control, and financial-crime frameworks administered by competent authorities including, inter alia, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the European Union and its Member States, the United Kingdom (HM Treasury / OFSI), the United Arab Emirates (Central Bank and other Competent Authorities), and the United Nations Security Council. It further incorporates the principles of international Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) regulation insofar as these intersect with sanctions screening, financial-crime prevention, and the detection or reporting of suspicious activity.

1.3 The Company recognises its statutory and ethical duty to deter, detect, and prevent any act or attempt of sanctions evasion, circumvention, or financial-crime abuse, including misuse of payment channels, escrow facilities, or affiliate structures. Through this Policy the Company declares its commitment to maintaining a risk-based, technology-assisted compliance framework proportionate to its Aggregator role, and to implementing adequate procedures that promote legality, transparency, and prudence while preserving operational flexibility to address emerging risks and regulatory developments.

1.4 This Policy forms part of the Company's broader Regulatory & Integrity Architecture, complementing its AML & CFT, Privacy, Data Security, and Escrow governance layers. It defines:

(a) the principles and scope of the Company's Sanctions Compliance Framework, including screening mechanisms, restricted-jurisdiction controls, and anti-circumvention rules;

(b) the structure of the Anti-Fraud Framework, encompassing detection, escalation, and proportionate mitigation of fraudulent conduct;

(c) the representations, warranties, and covenants expected of Users and counterparties to ensure lawful participation in the Company's ecosystem;

(d) the rights and remedial measures reserved to the Company, such as the suspension, blocking, or freezing of transactions where risk indicators are identified, together with its duties of cooperation with competent authorities under Applicable Law; and

(e) the governance, accountability, and review mechanisms through which the Policy is administered, periodically audited, and updated to maintain consistency with international best practice.

1.5 For the avoidance of doubt, this Policy serves as a public statement of commitment and interpretive summary of the Company's internal compliance operations. It does not disclose or confer operational detail regarding investigative procedures, escalation matrices, or reporting protocols, which remain confidential within the internal manuals of the Company. Nothing herein shall be construed as limiting any statutory or regulatory obligations of the Company under Applicable Law, nor as waiving any right or remedy available to it in law or equity.

1.6 Users, Affiliates, and Partners engaging with any of the Company's Services are deemed to have read, understood, and accepted this Policy in conjunction with the Terms of Service and related documents. By continuing to access or utilise the Services, each User acknowledges the Company's authority to apply, enforce, and adapt the controls described herein in accordance with Applicable Law and legitimate compliance objectives.

2. DEFINITIONS

2.1 Capitalised Terms. The capitalised terms used in this Policy shall bear the meanings set out below, mutatis mutandis, and shall be construed consistently with the Company's other public-facing policies and applicable compliance frameworks, including its user terms, data-protection, information-security, and financial-crime-prevention standards, save where expressly stated otherwise.

2.2 Applicable Sanctions Laws. Means, collectively, all binding sanctions, export-control and trade-restriction laws, regulations, directives and official interpretations issued by any Competent Authority having jurisdiction over the Company or the relevant transaction, including the OFAC programmes and Specially Designated Nationals List ("SDN List"), the EU Consolidated List, the UK Financial Sanctions Regime, the UAE Sanctions Measures, and any UN Security Council regimes, together with any amendments or successors thereto.

2.3 Sanctioned Person. Means any natural or legal person (including any individual, entity, vessel, aircraft or digital-asset address) that (i) appears on, is owned or controlled (by ≥ 50 percent) by, or acts for the benefit of a person appearing on any applicable sanctions list; or (ii) is located in, organised under the laws of, or ordinarily resident in a Restricted Jurisdiction; or (iii) is otherwise the subject of Applicable Sanctions Laws.

2.4 Restricted Jurisdiction. Means any country or territory subject to comprehensive embargo or territorial sanctions under Applicable Sanctions Laws, as periodically listed and maintained within the Company's internal Sanctions Register and publicly referenced in Schedule 1 (Restricted Jurisdictions & Lists).

2.5 Prohibited Transaction. Means any transaction or arrangement that would breach Applicable Sanctions Laws or facilitate such a breach, including transactions with or for the benefit of a Sanctioned Person, or any scheme to evade or circumvent sanctions or trade controls.

2.6 Financial Fraud. Means any fraudulent or abusive use of payment systems, escrow facilities, or identity-verification controls (for example, stolen instruments, synthetic identities, mule activity, affiliate manipulation, bot-driven traffic), but excludes ordinary delivery disputes regulated under the Terms of Service unless intrinsically linked to financial-crime conduct.

2.7 Services. Means the Company's websites, platforms, white-label storefronts, APIs, escrow mechanisms and ancillary functions through which in-game transactions are initiated, processed or settled.

2.8 Affiliate. Means any entity directly or indirectly controlling, controlled by, or under common control with the Company, where "control" denotes ownership of more than fifty percent (> 50 %) of voting interests.

2.9 AML and CFT Policy. Means the Company's separate policy governing anti-money-laundering and counter-terrorist-financing controls (including KYC/CDD/EDD processes, transaction monitoring and suspicious-activity reporting), which shall be read together with this Policy, mutatis mutandis.

2.10 Beneficial Owner. Means the natural person(s) who ultimately owns or controls a User or on whose behalf a transaction is conducted, including those exercising ultimate effective control over a legal person or arrangement.

2.11 Customer Due Diligence (CDD). Means the baseline identification and verification procedures applied to Users in accordance with FATF Recommendation 10.

2.12 Enhanced Due Diligence (EDD). Means additional verification or documentation steps applied to higher-risk Users, Sanctioned Persons, Restricted Jurisdictions, or complex transactions.

2.13 Know-Your-Customer (KYC). Means the process by which the Company identifies and verifies its Users or counterparties, including collection and validation of identity and ownership information.

2.14 Risk-Based Approach (RBA). Means the methodology whereby the Company applies proportionate controls commensurate with the identified level of sanctions or fraud risk, in line with FATF Recommendation 1.

2.15 Competent Authority. Means any governmental, regulatory, supervisory or enforcement body (including OFAC, EU authorities, HM Treasury/OFSI, the UAE Central Bank, the United Nations Security Council, financial-intelligence units or their successors) having lawful jurisdiction over the Company, its Services, its Users or its Affiliates.

2.16 Suspicious Transaction Report (STR) / Suspicious Activity Report (SAR). Means a mandatory report to Competent Authorities where there are reasonable grounds to suspect that funds or transactions may be linked to money-laundering, terrorist-financing, sanctions breaches or fraud, without reference to specific internal filing formats or systems.

2.17 Risk Indicators / Red Flags. Means patterns, behaviours or circumstances identified by the Company or in competent-authority guidance as potentially indicative of sanctions evasion or fraudulent activity.

2.18 Personal Data. Means any information relating to an identified or identifiable natural person, processed in accordance with the Company's Privacy & Cookie Policy and Applicable Law.

2.19 User. Means any Buyer, Seller, Influencer, Affiliate or other person accessing or using the Services, including their representatives, employees or assigns.

3. SCOPE, INTERPRETATION & HIERARCHY

3.1 Scope (Coverage).
This Policy applies, mutatis mutandis, to all activities undertaken by or on behalf of the Company that may expose the Company, its Affiliates, Subsidiaries, counterparties or Users to sanctions risk or Financial Fraud.

3.1.1 Without limitation, such activities include onboarding, KYC/CDD/EDD procedures, sanctions-list screening, payment processing, transaction routing, escrow administration, reconciliation, refunds or chargebacks, payout operations, affiliate remuneration, and fraud monitoring across the Services.

3.1.2 This Policy forms an integral component of the Company's overarching Financial-Crime Prevention Framework and shall be interpreted consistently therewith.

3.2 Relationship to AML/CFT.
While AML/CFT controls are addressed comprehensively in the Company's AML & CFT Policy, the sanctions-screening, sanctions-evasion detection and Financial-Fraud safeguards established herein constitute complementary mechanisms within that broader framework.

3.2.1 In the event of overlap or tension, each policy shall prevail with respect to its defined remit.

3.2.2 Where standards diverge, the stricter or more risk-sensitive standard shall apply.

3.3 Aggregator Role Disclaimer.
The Company acts solely as an Aggregator and technical facilitator, and not as the originator, owner, or provider of the underlying digital goods or services.

3.3.1 Nothing herein shall be construed to create obligations of performance with respect to third-party goods or services.

3.3.2 Any such obligations arise only where expressly mandated under Applicable Law or contractually assumed by the Company.

3.4 Territorial Reach.
This Policy applies extraterritorially, to the maximum extent permitted by Applicable Law, to all jurisdictions in which the Company's Services are accessed, targeted, or may otherwise give rise to sanctions or fraud risk.

3.4.1 Such extraterritorial application shall be construed subject to conflicts-of-law principles, mandatory local public policy, and the overriding discretion of Competent Authorities.

3.5 Carve-Outs & Limitations.
Notwithstanding the foregoing, this Policy shall not apply to:

3.5.1 hypothetical or demonstrative transactions devoid of legal or economic effect;

3.5.2 activities expressly exempted under Applicable Law (to be narrowly construed); or

3.5.3 activities occurring exclusively on external peer-to-peer platforms not integrated into the Company's infrastructure, save where the Company is contractually or legally compelled to extend oversight thereto.

3.6 Interpretation & Hierarchy.
In any conflict between this Policy and any annex, schedule or exhibit, the annex, schedule or exhibit shall prevail solely in relation to its specific subject matter.

3.6.1 References herein to "including" or "inter alia" shall mean "including, without limitation."

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

3.6.3 Words importing the singular shall include the plural and vice versa.

3.7 Language & Authentic Version.
Translations of this Policy are provided for convenience only.

3.7.1 The English version shall be authoritative and controlling, except where mandatory local law requires otherwise.

3.8 Current Version Clause.
For the avoidance of doubt, any references in this Policy to other Company policies or documents shall refer to the current and publicly available versions thereof, as may be updated from time to time.

3.8.1 The latest version published on the Company's official website shall at all times be deemed the authoritative and applicable version for public reference, without prejudice to any internal compliance documentation maintained separately by the Company.

4. SANCTIONS COMPLIANCE FRAMEWORK

4.1 Risk-Based Approach.
The Company shall, subject always to Applicable Sanctions Laws, proportionality, and the principles of necessity and prudence, implement and maintain a dynamic, risk-based sanctions-compliance framework.

4.1.1 Such framework shall consist of, inter alia:

(a) screening of counterparties (natural and legal persons), Beneficial Owners, payment instruments and, where proportionate, device, network and behavioural indicators;

(b) geo-location, IP and network controls designed to restrict or deter access from Restricted Jurisdictions and to identify evasion typologies;

(c) alert generation, review, escalation and disposition procedures proportionate to the nature and severity of identified risk; and

(d) periodic reassessment of sanctions-risk indicators in line with Competent-Authority guidance and industry best practice.

4.2 Screening.
The Company may conduct sanctions screening, directly or through vetted providers, at onboarding, transaction execution, payout and periodically thereafter, against applicable consolidated sanctions lists.

4.2.1 Screening shall, where feasible, extend to ownership and control relationships consistent with EU/UK prohibitions on making funds or economic resources available to listed persons or for their benefit.

4.2.2 While the Company makes no representation or warranty as to the detection of all potential matches, it shall act diligently and in good faith to identify and escalate potential matches in accordance with Applicable Sanctions Laws.

4.3 Restricted Jurisdictions.

Access to the Services by or on behalf of persons located in, organised under the laws of, or ordinarily resident in Restricted Jurisdictions is prohibited, save where expressly permitted by Applicable Sanctions Laws, general licences or specific authorisations issued by a Competent Authority.

4.3.1 The Company may, on a risk-sensitive basis, apply enhanced monitoring or access controls to neighbouring jurisdictions or high-risk corridors where elevated evasion or circumvention risk is observed.

4.4 Circumvention.

Users shall not, directly or indirectly, engage in, facilitate, cause, or attempt to engage in any activity the purpose or effect of which is to evade, bypass, frustrate or otherwise circumvent Applicable Sanctions Laws.

4.4.1 Prohibited circumvention includes, without limitation, the use of VPNs, anonymisers, proxies, straw persons, intermediate accounts, trans-shipment practices, or falsification or misrepresentation of location, identity or ownership.

4.5 Holds, Refusals and Blocking.

The Company may, notwithstanding any contrary provision and without prior notice, acting reasonably and in good faith:

4.5.1 decline, delay, freeze, block, reverse or refuse any transaction or payout;

4.5.2 restrict, suspend or terminate User access to the Services; and/or

4.5.3 place funds on administrative, technical or regulatory hold pending review or clearance,

where the Company determines on reasonable grounds that sanctions risk, Financial-Fraud risk or circumvention activity may be present.

4.6 Freeze Without Delay; Reporting.

Where a confirmed or potential sanctions match is identified, the Company shall freeze or suspend any relevant funds, instruments or transactions without delay.

4.6.1 The Company shall report such freezing action, attempted transaction or suspicious activity to the Competent Authorities of the relevant jurisdiction in accordance with Applicable Sanctions Laws.

4.6.2 Without prejudice to confidentiality or data-protection obligations, the Company shall co-operate with such authorities in good faith and within statutory timelines.

4.7 U.S. OFAC Risk-Based Program.
To the extent that a U.S. nexus may arise — including the use of U.S. financial institutions, U.S. persons or USD-denominated transactions — the Company shall align its sanctions-compliance program with the risk-based framework articulated by the U.S. Office of Foreign Assets Control (OFAC).

4.7.1 Such alignment encompasses management commitment, risk assessment, internal controls, independent testing or audit, and training.

4.7.2 Nothing herein shall create an obligation to adopt or maintain any specific control for any duration beyond what is proportionate and required by Applicable Sanctions Laws.

4.8 Governance, Records and Auditability.
All sanctions-related alerts, escalations, dispositions, holds and reports shall be logged and retained in accordance with the Company's internal record-keeping and audit standards.

4.8.1 The Company shall maintain auditable records of compliance decisions and ensure periodic testing of control effectiveness.

4.8.2 Relevant personnel shall receive training proportionate to their role in sanctions-compliance oversight.

5. FINANCIAL FRAUD (COMPLIANCE CONTEXT)

5.1 Scope Limitation.
For the avoidance of doubt, this Section addresses Financial Fraud in the sense of abuse of payment rails, escrow mechanisms, onboarding/KYC controls, and identity verification, and not the merits of in-game item delivery or fulfilment disputes, which are governed under the Terms of Service, Escrow & Payment Policy, and Prohibited Items & Restricted Activities Policy.

5.2 Illustrative Behaviours.
Without limitation and subject always to Applicable Law, Financial Fraud shall be deemed to include the following typologies:

5.2.1 use of stolen, compromised, or unauthorised payment instruments (cards, wallets, payment tokens, or crypto addresses);

5.2.2 identity fabrication, impersonation, or document forgery during KYC/CDD/EDD onboarding;

5.2.3 collusive behaviour between counterparties to simulate, wash, layer, or cycle funds;

5.2.4 mule activity or use of intermediaries designed to obscure the true Beneficial Owner or origin of funds;

5.2.5 structured, fragmented, or otherwise manipulated transactions intended to defeat monitoring thresholds, sanctions, or AML/CFT reporting obligations; and

5.2.6 submission of knowingly false chargebacks, refund claims, or misrepresentations of delivery, identity, or transaction status, whether for personal gain or to facilitate third-party fraud.

5.3 Controls.
The Company may implement, adapt, and retire from time to time proportionate and reasonable controls, including without limitation:

5.3.1 velocity limits and transaction caps;

5.3.2 behavioural, contextual, and device-level risk scoring;

5.3.3 step-up authentication and verification measures;

5.3.4 cooling-off periods, escrow extensions, and settlement delays; and

5.3.5 manual review, hold, or escalation to senior Compliance personnel.

The nature, scope, and configuration of such controls shall be operational in character, risk-based, and subject to ongoing adjustment. Nothing herein shall be construed as a binding commitment to adopt or maintain any specific measure for any duration beyond what is proportionate, practicable, and required by Applicable Law.

5.4 Monitoring & Escalation.

Financial-Fraud alerts and anomalies shall be subject to layered review, escalation, and documentation procedures consistent with the Company's AML & CFT Policy.

5.4.1 Escalations may result in holds, declines, suspensions, or STR/SAR filings to Competent Authorities, subject always to applicable "no-tipping-off" obligations.

5.5 Governance, Records & Auditability.

All Financial-Fraud controls, alerts, escalations, outcomes, and reports shall be logged, retained, and auditable in accordance with the Company's internal record-keeping and audit standards.

5.5.1 The Company shall periodically review fraud typologies, update its controls framework, and ensure appropriate governance oversight to preserve proportionality, effectiveness, and accountability.

5.6 Training & Awareness.

Relevant employees, contractors, and service providers shall receive proportionate training on emerging fraud typologies, detection methods, escalation channels, and reporting obligations, consistent with OFAC/AML guidance and industry standards, to ensure continual improvement of the Financial-Fraud compliance framework.

SECTION 6 — USER REPRESENTATIONS, WARRANTIES & COVENANTS

6.1 No Sanctions Exposure.

Each User hereby represents, warrants and covenants, on a continuing basis, that they:

6.1.1 are not a Sanctioned Person;

6.1.2 are not located in, established under the laws of, or ordinarily resident in any Restricted Jurisdiction; and

6.1.3 are not acting, directly or indirectly, for or on behalf of any Sanctioned Person or other person subject to restrictions under Applicable Sanctions Laws.

Users further covenant not to engage in any transaction, activity, or arrangement that would reasonably be expected to expose the Company, its Affiliates, or partners to sanctions liability, enforcement risk, or reputational harm under Applicable Sanctions Laws.

6.2 Lawful Funds.
Each User represents, warrants and covenants that all funds, assets, payment instruments, or other value used in connection with the Services are derived from lawful, legitimate, and verifiable sources.

6.2.1 Users shall not, directly or indirectly, use or permit the use of any funds for the purpose of financing, supporting, or concealing any unlawful conduct, including but not limited to sanctions evasion, terrorist financing, money laundering, Financial Fraud, tax evasion, corruption, or other financial crime.

6.2.2 The Company reserves the right to verify and validate the origin of funds, instruments, or assets at any time as part of its compliance and risk-management framework.

6.3 Accuracy of Information.
Users represent and warrant that all information, documentation, and certifications supplied to the Company (whether during onboarding, transaction execution, payout, or thereafter) are true, complete, accurate, and not misleading in any material respect.

6.3.1 Users covenant to promptly update such information upon any material change, including but not limited to changes in ownership, residency, control, sanctions exposure, or Beneficial Ownership.

6.3.2 Failure to provide accurate, current, and verifiable information shall constitute a material breach of this Policy and may result in suspension, termination, or withholding of funds under the Escrow & Payment Policy.

6.4 Cooperation.
Users shall promptly provide such information, documentation, certifications, or clarifications as the Company may reasonably request to assess or verify sanctions, Financial Fraud, or other compliance risks.

6.4.1 Users shall cooperate fully with the Company in any review, audit, remediation, investigation, or reporting activity undertaken in connection with this Policy or with Applicable Law.

6.4.2 Failure to cooperate may result in suspension of account access, delay in payout or fulfilment, and reporting to Competent Authorities in accordance with Applicable Law.

6.5 Undertaking Not to Circumvent.
Users covenant not to engage in, attempt, cause, or facilitate any circumvention of Applicable Sanctions Laws, Financial-Crime controls, or the Company's compliance procedures.

6.5.1 Prohibited conduct includes, without limitation, the use of VPNs, proxies, anonymisers, straw persons, nominee arrangements, layering, token intermediaries, false declarations, or other subterfuge designed to disguise true identity, location, or transaction purpose.

6.5.2 The Company may, acting in good faith, implement technical, analytical, or behavioural controls to detect and prevent such circumvention attempts.

6.6 Acknowledgement of Remedies.
Users acknowledge and agree that any breach of the foregoing representations, warranties, or covenants shall constitute a material breach of this Policy and of the Terms of Service.

6.6.1 Such breach may result, without prejudice to any other rights of the Company, in:

(a) suspension or termination of access to the Services;

(b) blocking, forfeiture, or delay of funds under the Escrow & Payment Policy;

(c) enhanced scrutiny, audit, or risk review; and

(d) mandatory reporting to Competent Authorities, consistent with AML/CFT and sanctions-reporting obligations.

6.6.2 Remedies exercised by the Company under this Section shall be without prejudice to any additional civil, contractual, or criminal liabilities of the User under Applicable Law.

7. ENFORCEMENT, REPORTING & COOPERATION WITH AUTHORITIES

7.1 Enforcement Actions.

In addition to any other remedies available at law, in equity or in contract, the Company may, acting reasonably and in good faith, and without prior notice where legally required:

7.1.1 suspend, restrict or terminate User accounts;

7.1.2 decline, freeze, cancel, reverse or otherwise restrict transactions, payouts or escrow releases;

7.1.3 withhold, offset or claw back commissions, remuneration or other payments; and

7.1.4 impose enhanced monitoring, conditional access or restrictions on future use of the Services,

where sanctions or Financial-Fraud risk is identified or reasonably suspected, or where a breach of User representations, warranties or covenants under Section 6 is discovered.

7.2 Mandatory & Voluntary Disclosures.

The Company may, subject to Applicable Law and confidentiality obligations, disclose information to Competent Authorities, including but not limited to governmental, supervisory, law enforcement, judicial, financial intelligence, sanctions enforcement, payment service providers, banks or partner platforms, for the purposes of compliance, investigation or enforcement.

7.2.1 Where required, the Company shall notify such authorities — inter alia, the Office of Financial Sanctions Implementation (OFSI) in the United Kingdom, the Office of Foreign Assets Control (OFAC) in the United States, the UAE Executive Office via the goAML platform, EU competent authorities, or other relevant national regulators — of frozen assets, suspected breaches or attempted transactions, in accordance with the forms, methods and timelines prescribed by such authorities.

7.3 International Cooperation.

To the extent permitted under Applicable Law, the Company may share relevant information with counterpart financial institutions, payment processors, partner platforms or regulators in other jurisdictions to prevent, deter and investigate sanctions breaches and Financial Fraud,

7.3.1 subject always to confidentiality, data-protection obligations and proportionality; and

7.3.2 ensuring such exchanges are undertaken in good faith and in accordance with recognised cooperation protocols or memoranda of understanding, where applicable.

7.4 No Tipping-Off.
Users acknowledge and agree that the Company may be legally prohibited from providing details of certain investigations, escalations, disclosures or enforcement actions, and may act without prior notice where legally required.

7.4.1 Any failure by the Company to inform a User shall not constitute a waiver of rights or remedies under this Policy or Applicable Law.

7.4.2 The Company shall, to the extent permitted, balance transparency with the need to preserve the integrity of ongoing compliance and enforcement measures.

7.5 Records & Auditability.
All enforcement actions, escalations, disclosures and cooperation measures undertaken pursuant to this Section shall be documented, retained and auditable in accordance with the Company's Internal Audit & Compliance Policy, statutory retention obligations and applicable no-tipping-off requirements.

7.5.1 Such records shall form part of the Company's Financial-Crime Prevention evidence framework and may be made available to Competent Authorities upon lawful request.

8. DATA PROTECTION & CONFIDENTIALITY

8.1 Privacy Policy.
Processing of Personal Data in the course of sanctions and Financial-Fraud controls shall be conducted strictly in accordance with the Company's Privacy & Cookie Policy, Data & Information Security Policy, and Applicable Law, including without limitation the EU GDPR, UK GDPR, UAE PDPL, and relevant U.S. State Privacy Laws.

8.1.1 Such processing shall observe the principles of lawfulness, fairness, transparency, necessity, proportionality, data minimisation, purpose limitation and retention limitation.

8.1.2 Personal Data shall be processed only for legitimate compliance and risk-management purposes directly related to the prevention, detection and mitigation of sanctions or Financial-Fraud risks.

8.2 Retention.
Records relevant to sanctions and Financial-Fraud assessments may be retained for such periods as are:

8.2.1 expressly mandated by Applicable Law;

8.2.2 reasonably necessary for compliance with legal or regulatory obligations;

8.2.3 required for defence of claims, litigation or audits; or

8.2.4 necessary to enable co-operation with Competent Authorities.

Upon expiry of the applicable retention period, such records shall be securely deleted, anonymised or archived in accordance with the Company's retention schedule and internal governance protocols.

8.3 Confidentiality & Access Controls.
Access to Personal Data, alerts, escalations, STRs/SARs, enforcement actions and related records shall be strictly limited to authorised personnel with a demonstrable need-to-know, and subject always to confidentiality undertakings, segregation-of-duties and audit logging.

8.3.1 Unauthorised disclosure, duplication or use of such data is strictly prohibited and shall constitute a material breach of Company policy.

8.3.2 Internal systems shall ensure traceability of every access, modification or transmission of regulated information.

8.4 Cross-Border Transfers.
To the extent that Personal Data or enforcement records are transferred across jurisdictions for compliance, reporting or investigative purposes, such transfers shall be effected only on lawful bases, including adequacy decisions, Standard Contractual Clauses, the UK International Data Transfer Addendum (IDTA) or Addendum to the SCCs, or other equivalent safeguards recognised under Applicable Law.

8.4.1 All transfers shall remain subject to the principles of necessity, proportionality and minimal disclosure.

8.4.2 The Company shall document transfer justifications and implement supplementary measures where risk assessment so requires.

8.5 Auditability.
The Company shall maintain audit trails evidencing the collection, use, disclosure and retention of Personal Data in connection with sanctions and Financial-Fraud compliance.

8.5.1 Such processes shall be subject to periodic review under the Internal Audit & Compliance Policy to ensure ongoing lawfulness, accuracy and accountability.

8.5.2 Findings from such reviews shall form part of the annual Compliance Audit Plan and be made available to Competent Authorities upon lawful request.

9. DISCLAIMERS; LIMITATION OF LIABILITY

9.1 No Guarantee of Detection.
The Company does not represent, warrant, or guarantee that sanctions violations, Financial-Fraud activity, suspicious transactions, or circumvention attempts will in all cases be detected, prevented, intercepted, or remedied.

9.1.1 The Company's controls are implemented on a risk-based and proportionate basis, are subject to technological and operational limitations, and may generate both false positives and false negatives.

9.1.2 Users acknowledge and accept such limitations as inherent in the nature of compliance and risk-management systems.

9.2 Third-Party Platforms & Partners.
Without prejudice to any mandatory obligations under Applicable Law, the Company expressly disclaims responsibility and liability for the acts, omissions, systems, failures, or practices of

external marketplaces, payment service providers, banks, fulfilment partners, or other third parties over which it lacks ownership, operational control, or contractual responsibility.

9.2.1 Users acknowledge that such third parties may apply their own compliance standards, fraud controls and sanctions-screening frameworks.

9.2.2 The Company does not warrant or assume liability for such measures or their effectiveness.

9.3 Evolving Regulatory Guidance.
Users acknowledge that sanctions regimes, enforcement priorities and Financial-Fraud typologies are subject to continual change by Competent Authorities and standard-setting bodies.

9.3.1 The Company disclaims liability for reliance on any outdated guidance, provided however that it shall act in good faith to update its controls and frameworks within a reasonable period after such changes become publicly known or legally effective.

9.4 Force Majeure.
The Company shall not be held liable for any delay, failure, omission or disruption in performance of its obligations under this Policy where such event is caused, directly or indirectly, by acts of God, war, terrorism, embargo, sanctions expansion, regulatory prohibition, cyber-attack, telecommunications failure, power outage or any other event beyond the reasonable control of the Company.

9.5 Limitation of Liability.
To the maximum extent permitted by Applicable Law, the Company shall not be liable for indirect, incidental, consequential, exemplary or punitive damages arising out of or relating to this Policy.

9.5.1 The aggregate liability of the Company, if any, whether in contract, tort (including negligence), equity or otherwise, shall be limited as set forth in the Terms of Service, Escrow & Payment Policy and/or Privacy & Cookie Policy, mutatis mutandis.

9.6 Contractual Primacy.
In the event of conflict between this Section and the Terms of Service, the limitation-of-liability provisions of the Terms of Service shall prevail, except where non-waivable provisions of Applicable Law dictate otherwise.

9.6.1 Nothing herein shall exclude or limit any liability that cannot lawfully be excluded under Applicable Law.

10. GOVERNANCE, TRAINING & AUDIT

10.1 Oversight & Accountability.
The Company shall designate qualified personnel — including but not limited to a Compliance Officer or an equivalent function — responsible for the administration, supervision, and implementation of this Policy.

10.1.1 Such personnel shall oversee the escalation, investigation, remediation, and disposition of sanctions alerts, Financial-Fraud indicators, and related compliance matters.

10.1.2 Oversight responsibility shall be exercised subject always to the principles of independence, proportionality, confidentiality, and accountability.

10.1.3 Significant compliance matters may be escalated to senior management, the Audit Committee, or other governance bodies as appropriate, in accordance with the Company's corporate governance framework.

10.2 Training & Awareness.
Relevant employees, contractors, and service providers engaged in onboarding, payment processing, fraud monitoring, sanctions screening, or related compliance activities shall receive role-specific training commensurate with their functions.

10.2.1 Training shall cover, inter alia:

(a) Applicable Sanctions Laws, AML/CFT principles, and Financial-Fraud typologies;

(b) escalation and reporting procedures, including STR/SAR and sanctions-match handling;

(c) no-tipping-off and confidentiality obligations; and

(d) updates to Competent-Authority guidance or industry best practices.

10.2.2 The frequency, scope, and format of such training shall be reviewed periodically and adapted to evolving risk profiles, regulatory developments, and internal audit findings.

10.2.3 Completion records and effectiveness assessments shall be maintained in accordance with the Internal Audit & Compliance Policy.

10.3 Audit, Review & Continuous Improvement.
This Policy, together with associated procedures, shall be subject to periodic review, internal audit, and where applicable, external assurance, either at the Company's discretion or where required by Applicable Law, contract, or Competent-Authority directive.

10.3.1 Reviews shall assess the design, adequacy, and operational effectiveness of sanctions and Financial-Fraud controls, including alert handling, escalation efficiency, and documentation integrity.

10.3.2 Audit findings shall inform corrective action plans, resourcing decisions, and framework enhancements, ensuring continuous improvement and proportionality of compliance controls.

10.3.3 Audit trails, findings, and remediation actions shall be documented and retained in accordance with the Internal Audit & Compliance Policy, and lessons learned shall be incorporated into the Company's broader risk-management and compliance frameworks.

11. AMENDMENTS; GOVERNING LAW; DISPUTE RESOLUTION

11.1 Amendments.
The Company may amend, modify, supplement or replace this Policy from time to time, with or without prior notice to Users where permitted by Applicable Law.

11.1.1 Material changes affecting User rights or obligations shall, where reasonably practicable, be notified through appropriate channels, including but not limited to email, platform notices or publication on the Company's website.

11.1.2 Continued use of the Services following such amendment shall constitute acceptance of the updated Policy.

11.2 Governing Law.
This Policy and any non-contractual obligations arising out of or in connection herewith shall be governed by and construed in accordance with the laws of the United Arab Emirates, specifically those in force in the Emirate of Fujairah, without regard to conflicts-of-law principles.

11.2.1 Mandatory provisions of other jurisdictions — including, inter alia, EU/UK data-protection, U.S. federal or state privacy law, or local sanctions laws with extraterritorial effect — shall apply to the extent not waivable by contract.

11.3 Jurisdiction & Relief.
Subject to Applicable Law and any non-waivable statutory carve-outs, the courts of Fujairah, United Arab Emirates, shall have exclusive jurisdiction to adjudicate any dispute arising from or in connection with this Policy.

11.3.1 Nothing herein shall preclude the Company from seeking injunctive, interim, equitable or conservatory relief in any court of competent jurisdiction.

11.3.2 The Company may, at its discretion, cooperate with Competent Authorities or enforcement bodies in multiple jurisdictions where compliance or investigative coordination is required.

11.4 Entire Agreement; Severability; No Waiver.
This Policy constitutes, with respect to its subject matter, the entire agreement between the Company and Users and supersedes any prior understandings, statements or representations to the extent permitted by law.

11.4.1 If any provision herein is held invalid, illegal or unenforceable, the remaining provisions shall continue in full force and effect, mutatis mutandis.

11.4.2 Failure or delay by the Company in enforcing any provision of this Policy shall not constitute or be construed as a waiver of such provision or of any other rights.

11.5 Survival & Binding Effect.
The obligations relating to enforcement, cooperation with authorities, confidentiality, limitation of liability, governing law and jurisdiction shall survive termination, suspension or expiry of this Policy and remain binding upon Users.

11.5.1 This Policy shall be binding upon and inure to the benefit of the Company, its Affiliates, successors and assigns.

11.6 Language.
This Policy is drafted in the English language.

11.6.1 Translations may be provided for convenience only; in the event of any inconsistency, the English version shall prevail, except where mandatory local law requires otherwise.

SCHEDULE 1 — RESTRICTED JURISDICTIONS & LISTS

S1.1 Dynamic Incorporation.
The Company dynamically incorporates by reference, as amended from time to time, the consolidated sanctions lists published by:

(a) the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC"), including, without limitation, the Specially Designated Nationals and Blocked Persons List (SDN) and applicable sectoral sanctions lists;

(b) the European Union;

(c) the United Kingdom, including the consolidated lists maintained by HM Treasury and the Office of Financial Sanctions Implementation ("OFSI");

(d) the United Arab Emirates; and

(e) the United Nations Security Council.

Such incorporation extends to any successor instruments, amendments, interpretive guidance or consolidated updates issued by the respective Competent Authorities.

S1.2 Nature of Incorporation.
This dynamic reference shall be illustrative and non-exhaustive, ensuring that the Company's Sanctions & Fraud Compliance controls remain aligned with evolving international obligations. The incorporated lists are self-updating through official publication by the relevant Competent Authorities, and Users are cautioned to rely exclusively on those official sources for current and authoritative information.

S1.3 Non-Exhaustive Illustration.
Without prejudice to S1.1, jurisdictions, territories or regions currently subject to comprehensive or near-comprehensive territorial restrictions under widely applied sanctions regimes may include, inter alia, such countries or regions as may from time to time be designated under U.S., EU, UK, UAE or UN law. This illustration is indicative only and does not constitute an authoritative or exhaustive list.

S1.4 Precedence; Licences.
Where a general or specific licence or authorisation is issued under Applicable Sanctions Laws, the Company may, at its sole discretion and subject always to risk-based proportionality, process a transaction or permit access under the terms of such licence. Nothing herein shall oblige the Company to process any transaction where material sanctions or Financial-Crime risk persists. In the absence of such a licence, Prohibited Transactions shall be declined, blocked, frozen or reported in accordance with this Policy and Applicable Law.

S1.5 User Responsibility.
Users acknowledge and agree that they remain independently responsible for ensuring their own compliance with Applicable Sanctions Laws, including verifying that they are not resident in, established under the laws of, or otherwise subject to restrictions relating to a Restricted Jurisdiction. The Company accepts no liability for any reliance placed on illustrative or outdated

references contained herein, and Users are expressly advised to consult current official lists as published by the respective Competent Authorities.

S1.6 Confidential Internal Annex (Non-Public).
For clarity, the Company maintains an internal Sanctions Register and procedural documentation specifying review cadence, alert escalation criteria and record-keeping arrangements. Such materials are confidential and not published, to preserve the integrity of compliance operations and in accordance with the confidentiality and "no-tipping-off" requirements of FATF Recommendation 21 and corresponding UAE, EU, UK and U.S. regulations.