ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND SANCTIONS COMPLIANCE STATEMENT

Effective Date: 31 August 2026

1. Purpose and Scope

Global Gold DAO is committed to maintaining the integrity, transparency, and lawful use of its real-world asset products, tokenization services, digital asset infrastructure, and related technologies and services.

We prohibit the use of the Platform for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, bribery, corruption, tax crimes, trafficking, market abuse, concealment of criminal proceeds, or any other unlawful activity.

This Statement applies, as relevant, to all users, customers, investors, issuers, asset originators, borrowers, beneficial owners, wallet holders, counterparties, service providers, and other persons accessing or participating in the Platform or its products.

2. Compliance Framework

We maintain a risk-based anti-money laundering and counter-terrorist financing (“AML/CFT”) compliance framework designed to comply with applicable laws and regulatory requirements in the jurisdictions in which we operate or provide services.

Where appropriate, our framework takes into account internationally recognized standards, including recommendations and guidance issued by the Financial Action Task Force (“FATF”), applicable United Nations Security Council sanctions, and relevant national or regional regulatory requirements.

Where requirements differ between jurisdictions, we may apply additional or stricter controls. Access to certain products or services may be restricted or prohibited based on a user’s location, legal status, risk profile, or applicable law.

3. Customer and Business Due Diligence

Before establishing or continuing a business relationship, we may conduct customer identification and verification procedures, including Know Your Customer (“KYC”) and Know Your Business (“KYB”) checks.

Such procedures may include:

- Collecting and verifying all customers, including all related parties such as directors, authorized representatives, controlling persons, and ultimate beneficial owners where applicable;

- Assessment of purpose and intended nature of the business relationship;

- Understanding source of funds, source of wealth, and expected transaction activities;

- Collecting relevant information and supporting documents may be requested during onboarding or at any time thereafter.

Users must provide complete, accurate, current, and non-misleading information. We may request additional documents or explanations at any time and may suspend or refuse services where requested information is not provided or cannot be satisfactorily verified.

4. Risk Assessment and Enhanced Due Diligence

We assess financial crime risks associated with users, products, jurisdictions, distribution channels, wallet addresses, transaction patterns, counterparties, and underlying real-world assets.

Enhanced due diligence may be applied to higher-risk relationships or activities, including those involving politically exposed persons, their family members and known close associates, high-risk jurisdictions, complex ownership structures, unusual transaction patterns, self-custodied wallets, privacy-enhancing technologies, cross-border structures, assets whose ownership or source cannot be adequately verified, or any other risk elevating factors as detected through our ongoing compliance effort such as Know Your Transaction (KYT) or Transaction Monitoring (TM).

Enhanced measures may include obtaining additional identification information, sanctions screening, adverse media screening and regulatory/enforcement checks, verifying source of funds or wealth, imposing transaction limits, and conducting more frequent monitoring or reviews.

For issuers, asset originators, sponsors, borrowers, and other parties involved in the creation or administration of real-world asset products, we may conduct enhanced business due diligence, including verification of legal existence, ownership and control, beneficial ownership, business activities, regulatory status, source of assets, source of funds, and relevant litigation, enforcement, sanctions, and adverse media information.

5. Sanctions and Prohibited Parties

We may not conduct business relationships with or provide services to sanctioned individuals and entities under applicable sanctions and restricted-party lists, including, where applicable, United Nations Security Council sanctions lists, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) lists, European Union sanctions lists, and applicable national sanctions lists.

We may not enter business relationships with clients from restricted jurisdictions. Restricted jurisdictions comprise those subject to applicable sanctions, embargoes, or equivalent restrictive measures imposed by competent authorities.

We may not allow funds, that we know via Know Your Transaction (KYT) monitoring or KYC checks, to be the proceeds of a crime or to be used for financing terrorism or belonging to a criminal organization, to enter into a client business relationship - even if the crime or offence was committed abroad.

We screen relevant persons, entities, beneficial owners, counterparties, and wallet addresses against applicable sanctions, terrorism, law-enforcement, and other restricted-party lists.

No person may use the Platform if such use would violate applicable sanctions or trade restrictions. Users must not directly or indirectly transact for the benefit of a sanctioned, prohibited, or restricted person, entity, jurisdiction, organization, or wallet address.

Users must not conceal their location, identity, ownership, source of funds, transaction beneficiary, use intermediaries, nominees, virtual private networks, proxy services, mixers, tumblers, chain-hopping techniques, or similar methods to evade compliance controls.

6. Transaction and Monitoring

We may monitor both on-chain and off-chain activity on an ongoing basis. Such monitoring may include, without limitation, blockchain analytics, wallet screening, transaction monitoring, analysis of asset flows, geographic indicators, counterparty risks, unusual behavior detection, and identification of connections to suspected illicit activity.

We may use blockchain analytics, wallet screening, transaction monitoring, and other technology-enabled compliance tools.

Where appropriate, we may require users or counterparties to demonstrate ownership or control of a wallet address, including through cryptographic signing, controlled transfers, or other verification methods.

Where required or appropriate, we may collect, retain, verify, and transmit information relating to transaction originators and beneficiaries in accordance with applicable Travel Rule and funds-transfer requirements.

7. Suspicious Activity and Enforcement Measures

If we identify suspected, attempted, unusual, or potentially unlawful activity, we may take any action permitted by applicable law and technically available to us. Such action may include:

- Rejecting an application or transaction;

- Requesting additional information or supporting evidence;

- Delaying, restricting, blocking, or cancelling a transaction;

- Suspending or terminating access to the Platform;

- Restricting token usage, transfer, redemption, or withdrawal;

- Freezing or segregating assets where legally authorized and technically possible;

- Reporting suspicious activity to competent authorities; and

- Cooperating with regulators, courts, law-enforcement agencies, financial intelligence units, or other authorized bodies.

Where prohibited by law, we will not notify a user that a suspicious activity report has been filed or that an investigation is underway.

8. Record Keeping and Information Sharing

We may retain identification information, transaction records, wallet data, communications, risk assessments, investigation materials, and supporting documents for the period required by applicable law or reasonably necessary for compliance purposes. Where applicable law requires a specific minimum retention period, we will retain records for no less than that period.

Subject to applicable laws, including data protection and confidentiality requirements, we may share relevant information with affiliates, regulated financial institutions, virtual asset service providers, custodians, compliance vendors, professional advisers, auditors, insurers, regulators, law-enforcement bodies, or other authorized parties. Personal data is processed in accordance with our Privacy Policy and applicable data protection and privacy laws.

We implement reasonable administrative, organizational, and technical safeguards intended to protect compliance-related information from unauthorized access, loss, misuse, or disclosure.

9. User Responsibilities

Each user is responsible for ensuring that their use of the Platform complies with all laws applicable to them. Users must not use the Platform to hold, transfer, tokenize, purchase, sell, finance, conceal, or otherwise deal with assets derived from unlawful activity.

Users must promptly notify us of any material change to their identity, ownership, control, regulatory status, source of funds, wallet ownership, or transaction purpose. Acceptance of a user or transaction does not constitute confirmation that the activity is lawful in every jurisdiction.

10. Governance and Amendments

We may maintain internal controls, employee training, compliance testing, independent reviews, escalation procedures, and designated compliance responsibilities proportionate to the nature, scale, and risk profile of our business.

We reserve the right to amend this Statement at any time in response to legal, regulatory, technological, operational, or risk-related developments. This version is effective as of the Effective Date stated above and shall remain in effect until replaced by a later version.

Nothing contained in this Statement constitutes or shall be deemed to constitute a representation that Global Gold DAO is licensed, registered, authorized, or subject to supervision as a financial institution, virtual asset service provider, securities intermediary, fund manager, payment institution, or other regulated entity in all jurisdictions. The regulatory treatment of particular products and services may vary depending on the applicable jurisdiction.

This Statement is a general compliance statement and does not constitute legal, tax, investment, or regulatory advice. If any provision conflicts with mandatory applicable law, that law shall prevail to the extent of the conflict.