Sabika Gold AML Policy

1. Purpose

This Anti-Money Laundering and Counter-Terrorist Financing Policy sets out Sabika Gold's approach to preventing, detecting, and reporting money laundering, terrorist financing, fraud, sanctions breaches, and other financial crime risks.

Sabika Gold is committed to operating with integrity and maintaining controls designed to prevent misuse of its gold purchase, sale, holding, and redemption services.

2. Scope

This Policy applies to:

- Sabika Gold;
- Directors, officers, employees, contractors, and agents;
- Customers using Sabika Gold services;
- Relevant third-party service providers;
- All products, transactions, channels, and markets operated by Sabika Gold.

3. Business Model

Sabika Gold provides a digital service that allows eligible customers to buy, hold, sell, and, where available, redeem allocated gold.

The customer account is intended only for Sabika Gold-related gold activity. It is not designed for general payments, third-party transfers, remittance, or cash movement between customers.

This closed-loop structure is intended to reduce money laundering and misuse risk by limiting how funds can enter, be used, and exit the service.

4. Regulatory Commitment

Sabika Gold will maintain AML/CTF controls designed to comply with applicable laws, regulations, regulatory guidance, and international standards, including risk-based customer due diligence, transaction monitoring, sanctions screening, record keeping, and suspicious activity escalation.

Where requirements differ across applicable jurisdictions, Sabika Gold will seek to apply the higher standard where appropriate and legally required.

5. Governance and Responsibility

Sabika Gold will appoint a responsible compliance officer or Money Laundering Reporting Officer where required.

The compliance function is responsible for:

- Maintaining this AML Policy;
- Conducting business risk assessments;
- Approving customer risk methodology;
- Overseeing KYC and due diligence controls;
- Monitoring suspicious activity;
- Escalating and reporting suspicious activity where required;
- Maintaining AML records;
- Training relevant staff;
- Reviewing the effectiveness of AML controls.

Senior management is responsible for ensuring adequate resources, systems, and oversight for AML compliance.

6. Risk-Based Approach

Sabika Gold applies a risk-based approach to AML/CTF.

Customer, transaction, product, geography, delivery channel, and partner risks will be assessed to determine the appropriate level of due diligence and monitoring.

Risk factors may include:

- Customer nationality or residence;
- Customer occupation or business activity;
- Politically exposed person status;
- Sanctions exposure;
- Source of funds;
- Transaction size and frequency;
- Use of multiple payment methods;
- Unusual purchase or sale patterns;
- Rapid buying and selling;
- Redemption requests;
- High-risk jurisdictions;
- Inconsistent customer behaviour;
- Adverse media or fraud indicators.

7. Customer Due Diligence

Before allowing customers to use Sabika Gold services, Sabika Gold may collect and verify identity information.

For individuals, this may include:

- Full legal name;

- Date of birth;
- Nationality;
- National ID, Iqama, passport, or equivalent document;
- Mobile number and email address;
- Residential address;
- Selfie, liveness check, or biometric verification where appropriate;
- Bank account ownership verification;
- Occupation and source of funds information where required.

For businesses, where permitted, this may include:

- Commercial registration documents;
- Ownership and control structure;
- Ultimate beneficial owners;
- Authorised signatories;
- Business activity;
- Source of funds and source of wealth;
- Tax or regulatory information where required.

8. Enhanced Due Diligence

Sabika Gold may apply enhanced due diligence to higher-risk customers or transactions.

Enhanced due diligence may include:

- Additional identity verification;
- Source of funds or source of wealth documents;
- Bank statements or income evidence;
- Senior management approval;
- Additional sanctions, PEP, or adverse media checks;
- More frequent account reviews;
- Lower transaction limits;
- Manual review before purchase, sale, withdrawal, or redemption.

Enhanced due diligence may be required for:

- Politically exposed persons;
- Customers linked to high-risk jurisdictions;
- Unusual or high-value transactions;
- Customers with adverse media;
- Customers with complex or unclear source of funds;
- Customers whose activity does not match their profile;
- Customers requesting repeated rapid purchase and sale activity.

9. Sanctions Screening

Sabika Gold will screen customers and, where appropriate, related parties against applicable sanctions, terrorist, watchlist, politically exposed person, and adverse media databases.

Screening may occur:

- During onboarding;
- Before transactions;
- Before withdrawals or refunds;
- Before physical redemption;
- Periodically during the customer relationship;
- When sanctions lists or customer information change.

Sabika Gold will not knowingly provide services to sanctioned persons, prohibited parties, or persons subject to applicable restrictions.

10. Prohibited Activity

Customers must not use Sabika Gold for:

- Money laundering;
- Terrorist financing;
- Sanctions evasion;
- Fraud;
- Identity theft;
- Use of stolen funds;
- Market manipulation;
- Third-party fund movement;
- Layering of funds through gold transactions;
- Use of another person's bank account;
- Transactions on behalf of undisclosed third parties;
- Any activity prohibited by law or Sabika Gold policy.

11. Transaction Monitoring

Sabika Gold may monitor customer activity to detect suspicious or unusual behaviour.

Monitoring may include:

- Transaction size;
- Transaction frequency;
- Rapid purchase and sale activity;
- Unusual funding patterns;
- Repeated failed payments;
- Refund patterns;
- Bank account mismatches;
- Unusual redemption requests;
- Structuring or splitting transactions to avoid limits;
- Use of multiple accounts or devices;
- Activity inconsistent with customer profile.

Alerts may be reviewed manually or automatically.

12. Source of Funds and Source of Wealth

Sabika Gold may request evidence of source of funds or source of wealth where required.

Examples of acceptable evidence may include:

- Salary records;
- Bank statements;
- Business income records;
- Sale agreements;
- Inheritance documents;
- Investment statements;
- Other documents reasonably required by Sabika Gold.

Failure to provide satisfactory evidence may result in transaction delay, account restriction, refusal of service, account closure, or reporting where required.

13. Payment Controls

Sabika Gold may require that funds used to buy gold come from a payment method or bank account in the customer's own name.

Sabika Gold may reject third-party payments, cash deposits, unusual payment flows, mismatched bank accounts, or transactions that cannot be properly verified.

Sale proceeds, refunds, or withdrawals may be paid only to a verified bank account in the customer's own name, unless otherwise approved and legally permitted.

14. Transaction Limits

Sabika Gold may apply limits based on customer risk, verification level, payment method, transaction type, account history, or regulatory requirements.

Limits may include:

- Purchase limits;
- Sale limits;
- Daily, weekly, monthly, or annual limits;
- Redemption limits;
- Available Balance to Buy Gold limits;
- Refund or proceeds transfer limits.

Sabika Gold may change limits at any time for legal, compliance, fraud prevention, operational, or risk management reasons.

15. Suspicious Activity Escalation

Employees and systems must escalate suspicious activity to the compliance function.

Examples of suspicious activity include:

- Refusal to provide identity or source of funds information;
- Use of inconsistent or false information;
- Attempted use of another person's bank account;
- Rapid purchase and sale activity without clear reason;
- Multiple accounts controlled by the same person;
- Transactions inconsistent with the customer's profile;
- Unusual redemption requests;
- Adverse media or sanctions indicators;
- Attempts to avoid limits or monitoring.

The compliance function will review alerts and determine appropriate action.

16. Reporting

Where Sabika Gold identifies suspicious activity that requires external reporting, it will report to the relevant authority in accordance with applicable law.

Sabika Gold will not notify the customer where doing so would breach applicable law or prejudice an investigation.

17. Record Keeping

Sabika Gold will maintain records of:

- Customer identification and verification;
- Due diligence and enhanced due diligence;
- Transaction history;
- Screening results;
- Risk assessments;
- Compliance reviews;
- Suspicious activity investigations;
- Reports made to authorities;
- Staff training;
- Policy approvals and updates.

Records will be retained for the period required by applicable law and internal policy.

18. Staff Training

Relevant staff will receive AML/CTF training appropriate to their role.

Training may cover:

- Money laundering and terrorist financing risks;
- Customer due diligence;
- Sanctions screening;

- Suspicious activity indicators;
- Escalation procedures;
- Confidentiality and tipping-off restrictions;
- Record keeping;
- Sabika Gold's internal policies and procedures.

19. Independent Review

Sabika Gold may conduct periodic internal or external reviews of its AML controls to assess effectiveness and identify improvements.

Reviews may cover:

- Customer onboarding;
- Transaction monitoring;
- Screening;
- Case management;
- Reporting;
- Record keeping;
- Governance;
- Staff training;
- Technology controls.

20. Third-Party Providers

Sabika Gold may use third-party providers for identity verification, sanctions screening, payment processing, transaction monitoring, and compliance support.

Sabika Gold remains responsible for maintaining appropriate oversight of outsourced AML-related services.

21. Breach of Policy

Any employee, contractor, customer, or partner who breaches this Policy may be subject to disciplinary action, account restriction, termination, reporting, or legal action.

22. Policy Review

This Policy will be reviewed periodically and updated where required due to changes in law, regulation, business model, risk assessment, products, systems, or operational requirements.