

GOLDEN TRADER

AML, CTF & SANCTIONS POLICY

Effective date	25 September 2026
Version	1.0
Jurisdiction	Saint Lucia

Our approach. Golden Trader applies proportionate, risk-based controls intended to prevent its accounts, trading platform and payment channels from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud or other financial crime. Verification may delay or prevent onboarding, deposits, withdrawals or continued access to services.

Golden Trader Ltd
Company No. 2025-00610
Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay,
Gros-Islet, Saint Lucia
<https://golden-trader.com>
Compliance enquiries: info@golden-trader.com

Contents

1. Purpose and scope
 2. Legal and policy framework
 3. Governance and responsibility
 4. Risk-based approach
 5. Customer due diligence
 6. Individual clients
 7. Corporate clients and beneficial ownership
 8. Enhanced due diligence
 9. Politically exposed persons
 10. Sanctions and restricted relationships
 11. Payments, withdrawals and crypto assets
 12. Ongoing monitoring
 13. Internal escalation and external reporting
 14. Account restrictions and termination
 15. Recordkeeping
 16. Staff awareness and training
 17. Outsourcing and reliance
 18. Data protection and confidentiality
 19. Client responsibilities
 20. Review and updates
- Schedule 1 - Risk factors and control responses
- Schedule 2 - Key definitions

This public policy summarises Golden Trader's financial-crime controls. It does not disclose confidential monitoring rules, alert thresholds, investigation methods or reporting decisions. It should be read with the Client Service Agreement, Privacy Notice, Deposit and Withdrawal Policy and Restricted Jurisdictions Policy.

1. Purpose and scope

1.1 This Policy describes the framework used by Golden Trader Ltd (the Company, Golden Trader, we, us or our) to identify, assess and manage risks relating to money laundering, terrorist financing, proliferation financing, sanctions, fraud and associated criminal conduct.

1.2 The Policy applies to applicants, clients, beneficial owners, directors, authorised persons, representatives, introducing brokers, affiliates, payments and activity conducted through the website, client portal, MT5 platform and approved communication or payment channels.

1.3 It applies throughout the relationship, from application and verification through trading, payments, withdrawals, account changes, periodic review and closure.

1.4 This is a public summary. Internal procedures may impose additional controls and may be changed without publishing operational details that could weaken detection or enable evasion.

2. Legal and policy framework

2.1 Golden Trader is incorporated and registered in Saint Lucia under Company No. 2025-00610. Incorporation does not itself constitute a financial-services licence or regulatory approval.

2.2 The Company seeks to act consistently with applicable laws of Saint Lucia concerning money laundering, terrorist financing, criminal property, sanctions and data protection, and with generally recognised risk-based financial-crime principles.

2.3 Where a legal duty applies to the Company, a transaction, a provider or a client relationship, that duty prevails over this Policy. Where no specific legal duty applies, the Company may still apply reasonable contractual controls to protect its services from misuse.

2.4 Nothing in this Policy represents that Golden Trader is licensed or supervised by the Financial Services Regulatory Authority of Saint Lucia for forex or CFD business.

3. Governance and responsibility

3.1 Senior management is responsible for approving the financial-crime framework, setting risk appetite, ensuring reasonable resources and reviewing material compliance matters.

3.2 The Company designates a person with responsibility for AML and financial-crime matters. That person coordinates risk assessment, due diligence standards, internal escalation, investigations, staff guidance, recordkeeping and external reporting where legally required.

3.3 Operational, onboarding, finance, support, sales, partnership and dealing personnel must follow approved procedures and escalate concerns. Commercial targets, seniority, referrals or personal relationships do not override required checks.

3.4 Material exceptions require documented approval from an authorised control function or senior management. An account manager, introducing broker or salesperson may not waive KYC, ownership, payment or sanctions requirements.

4. Risk-based approach

4.1 We assess financial-crime risk by considering the client, beneficial owners and controllers, geography, products, payment methods, delivery channel, expected trading and transaction behaviour, source of funds or wealth, use of intermediaries and other relevant information.

4.2 Risk is assessed at onboarding and may be reassessed periodically or when circumstances change. Higher risk does not automatically mean criminal activity, but it may require additional information, approval, monitoring, limits or refusal.

4.3 We may apply simplified operational steps only where risk is demonstrably lower and applicable requirements allow it. Core identity, sanctions and beneficial-ownership checks are not removed merely for convenience.

4.4 We do not disclose scoring models, monitoring scenarios, internal thresholds or vendor rules.

5. Customer due diligence

5.1 We do not knowingly maintain anonymous, fictitious or numbered-only client relationships. An account may not be activated for live trading or funding until the required verification is completed or an expressly approved exception permitted by law applies.

5.2 CDD includes identifying and verifying the client; identifying beneficial owners, controllers and authorised persons; understanding the purpose and expected nature of the relationship; screening relevant parties; and obtaining information on source of funds or wealth where appropriate.

5.3 Verification may use documents, electronic databases, biometric or liveness technology, public registers, sanctions and PEP data, payment records and other reliable independent sources.

5.4 We may request updated, clearer, translated, notarised, certified or additional documents where authenticity, validity, ownership, address, authority or risk cannot be established.

5.5 CDD is ongoing. Clients may be asked to refresh expired documents, explain activity, confirm tax residence, update occupation or business details, or substantiate a payment or withdrawal.

6. Individual clients

6.1 Information may include full legal name, date and place of birth, nationality, residential address, contact details, occupation, employer, tax residence, government identification, recent proof of address, expected account activity and payment details.

6.2 We may request source-of-funds evidence such as bank statements, payslips, business income records, sale agreements, investment statements or other documents reasonably connected to the proposed funding.

6.3 Where risk is higher, we may request source-of-wealth information explaining how the client's overall wealth was accumulated, together with supporting evidence.

7. Corporate clients and beneficial ownership

7.1 For a legal entity, we may obtain incorporation and constitutional documents, registered and operating addresses, business activity, ownership structure, directors, authorised persons, account purpose, expected activity, tax information, board approval and source-of-funds information.

7.2 We identify and take reasonable measures to verify each natural person who directly or indirectly owns 25% or more of the entity, and any natural person who otherwise exercises ultimate control regardless of ownership percentage.

7.3 If no individual meets the ownership threshold, we identify the person or persons exercising control through other means. If a controlling person cannot be identified after reasonable measures, we may identify an appropriate senior managing official while documenting the steps taken.

7.4 Complex, nominee, trust, foundation, partnership or multi-layer structures may require ownership charts, registers, declarations, trust documents, legal opinions or information about settlors, trustees, protectors, beneficiaries, partners or equivalent parties.

7.5 A relationship will not proceed where ownership or control is concealed, inconsistent or cannot be reasonably understood and verified.

8. Enhanced due diligence

8.1 Enhanced due diligence (EDD) is applied where the assessed risk is higher. It may include additional identity evidence, independent corroboration, deeper source-of-funds or wealth review, management approval, restrictions, more frequent review and enhanced monitoring.

8.2 EDD may be triggered by high-risk geography, political exposure, sanctions proximity, unusual ownership, cash-intensive or high-risk business, adverse information, use of intermediaries, unusual payment routes, significant or unexplained activity, digital-asset risk, or inconsistency with the stated profile.

8.3 The presence or absence of one factor is not decisive. We assess the relationship as a whole and may decline it even where individual documents appear valid.

9. Politically exposed persons

9.1 We take reasonable measures to determine whether a client, beneficial owner or controller is a politically exposed person (PEP), a family member or a known close associate.

9.2 PEP status does not automatically prohibit a relationship. It normally requires EDD, reasonable source-of-wealth and source-of-funds review, appropriate senior-management approval and ongoing monitoring.

9.3 Controls may continue after a person leaves public office for as long as risk remains. Clients must disclose relevant political exposure and changes promptly.

10. Sanctions and restricted relationships

10.1 We screen relevant clients, beneficial owners, controllers, authorised persons and, where appropriate, payments or wallet information against sanctions and restricted-party information from sources selected according to the relationship and applicable risk.

10.2 Screening may occur during onboarding, periodically and when a triggering event occurs, including a list update, ownership change, payment, profile change or potential match. We do not represent that every database is screened continuously in real time.

10.3 Sources may include United Nations, United States OFAC, United Kingdom, European Union and other national or international lists relevant to our business, providers or payment routes.

10.4 We may reject an application or transaction, restrict access, suspend processing, freeze or block assets where legally required, request information, or terminate a relationship where sanctions risk cannot be resolved.

10.5 We do not knowingly provide services intended to evade sanctions or geographic restrictions, including through proxies, nominees, false residence information, VPN misuse or third-party payment routes.

11. Payments, withdrawals and crypto assets

11.1 Golden Trader does not accept physical cash directly from clients. Funding and withdrawals must use approved, traceable channels such as bank transfer, supported card processing or an approved digital-asset wallet or payment provider.

11.2 Payments should originate from and be returned to an account, card or wallet held in the client's own name. Third-party funding and withdrawals are generally prohibited. A genuine exceptional arrangement must be disclosed in advance, independently verified, documented and expressly approved before use.

11.3 We may require proof of bank, card or wallet ownership; payment statements; transaction hashes; wallet screenshots or signatures; source-of-funds evidence; counterparty information; or an explanation of payment purpose.

11.4 Crypto-asset transactions may be reviewed using blockchain, wallet-risk or service-provider information. Exposure to theft, scams, mixers, darknet markets, sanctioned services, fraud or other high-risk activity may lead to delay, rejection, restriction or further investigation.

11.5 We may return funds through the original method before permitting another route and may delay processing while verification or investigation is reasonably required.

11.6 Trading activity does not cleanse or validate the source of funds. Rapid deposit-trade-withdrawal cycles, low-risk offsetting activity or use of the account mainly as a payment conduit may be reviewed.

12. Ongoing monitoring

12.1 We monitor the relationship on a risk-based basis to determine whether identity, ownership, payments, trading and account behaviour remain reasonably consistent with the known profile and expected purpose.

12.2 Monitoring may combine automated alerts, vendor information and manual review. It may consider changes in ownership, geography, devices, payment routes, transaction size or frequency, unusual trading patterns, linked accounts, adverse information and unexplained behaviour.

12.3 An alert is not proof of wrongdoing. It prompts review, which may include requesting information, comparing records, escalating internally or applying temporary controls.

12.4 We do not publish monitoring thresholds, scenarios or investigation methods.

13. Internal escalation and external reporting

13.1 Personnel must promptly report knowledge, suspicion or reasonable grounds for concern through the internal escalation route designated by the Company. The responsible person must have reasonable access to information needed to assess the matter.

13.2 The designated AML responsible person reviews escalations, records the basis for the decision and determines appropriate action, including further enquiry, account controls, termination or a report to a competent authority where legally required.

13.3 The Company will cooperate with lawful requests from courts, law-enforcement bodies, financial-intelligence authorities and other competent authorities, subject to applicable law and verification of the request.

13.4 Clients and unauthorised persons will not be informed that a suspicious transaction report, investigation or authority request has been made where disclosure is prohibited or could prejudice an investigation. This is commonly referred to as avoiding tipping off.

13.5 The Company is not required to explain confidential monitoring, legal reports, third-party intelligence or law-enforcement communications.

14. Account restrictions and termination

14.1 We may decline onboarding, refuse a payment, delay a withdrawal, limit transactions, request documents, suspend an account, close positions or terminate a relationship where due diligence is incomplete, risk is unacceptable, information is misleading, activity is unexplained or a legal or contractual restriction applies.

14.2 A restriction is not necessarily an allegation of criminal conduct. It may be required while facts are verified, a provider responds, a payment settles or legal advice is obtained.

14.3 Where permitted, remaining funds will be returned through an approved method after obligations and lawful restrictions are resolved. We may be unable to provide advance notice or detailed reasons in some cases.

15. Recordkeeping

15.1 As a company policy, core identity, ownership, due-diligence, screening, payment, trading, communication, investigation and decision records are generally retained for seven years after account closure or the end of the relationship.

15.2 Records may be retained longer where an investigation, payment dispute, complaint, litigation, authority request, sanctions measure or other lawful preservation reason applies.

15.3 Records should be sufficient to reconstruct relevant transactions and explain material onboarding, risk, restriction and reporting decisions.

16. Staff awareness and training

16.1 Relevant personnel receive proportionate instruction on identity and beneficial-ownership checks, PEPs and sanctions, payment controls, red flags, internal escalation, confidentiality, recordkeeping and the prohibition on tipping off.

16.2 Training and guidance are refreshed when roles, products, risks, systems or legal requirements materially change. Serious or repeated failure to follow controls may result in access restriction or disciplinary action.

17. Outsourcing and reliance

17.1 We may use third parties for identity verification, biometric checks, sanctions and PEP screening, fraud prevention, hosting, platform services, payments, wallet analysis and record storage.

17.2 Use of a provider does not remove the Company's responsibility for deciding whether to accept, restrict or end a relationship. A successful automated result does not guarantee acceptance.

17.3 Providers are selected and reviewed in a manner proportionate to their role, data access, security, reliability and the risks involved. We may replace a provider without amending this public Policy.

18. Data protection and confidentiality

18.1 Personal data collected for financial-crime purposes is handled in accordance with the Privacy Notice and applicable data-protection requirements. Access is limited according to role and business need.

18.2 Information may be shared with verification and screening vendors, banks, payment providers, platform and technology providers, advisers, counterparties and competent authorities where reasonably necessary or legally required.

18.3 Confidentiality does not prevent disclosure required by law or needed to report, investigate or prevent suspected criminal conduct.

19. Client responsibilities

19.1 Clients must provide accurate, complete and current information; respond reasonably to verification requests; disclose beneficial ownership and control; use payment methods they are authorised to use; and notify us promptly of material changes.

19.2 Clients must not submit false documents, conceal another person, structure activity to avoid checks, use the account for another person without approval, facilitate sanctions evasion, or use trading as a means to move or disguise funds.

19.3 Failure to cooperate may result in delayed onboarding or payments, account restriction, termination, return of funds where permitted, and reporting where legally required.

20. Review and updates

20.1 This Policy is reviewed periodically and when material changes occur in services, payment methods, systems, risk exposure or applicable law.

20.2 The current public version and effective date will be published on the Company's website. Internal procedures may be updated more frequently without public disclosure.

20.3 Compliance questions and document submissions may be sent to info@golden-trader.com. Do not send passwords or one-time authentication codes.

Compliance contact
Golden Trader Ltd
Company No. 2025-00610
Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia
Website: <https://golden-trader.com>
Email: info@golden-trader.com

Schedule 1 - Risk factors and control responses

Risk area	Examples	Possible response
Identity and document risk	Inconsistent, expired, altered, unverifiable or third-party information	Additional documents, independent verification, rejection or restriction
Ownership and control risk	Complex layers, nominees, unexplained control or hidden beneficial owners	Ownership chart, registers, declarations, EDD and management review
Geographic risk	Restricted, sanctioned, conflict-affected or higher-risk connections	EDD, limits, provider checks, refusal or sanctions controls
PEP and public-function risk	Client or connected person is politically exposed	Source-of-wealth/funds review, approval and enhanced monitoring
Payment risk	Third-party, mismatched, rapidly routed or unexplained payment activity	Ownership evidence, payment review, return to source, delay or rejection
Crypto-asset risk	High-risk services, obscured source, theft or sanctions exposure	Wallet and transaction review, evidence request, restriction or rejection
Behavioural risk	Activity materially inconsistent with profile or stated account purpose	Clarification, profile update, enhanced monitoring or investigation
Adverse information	Credible allegations involving fraud, crime, sanctions or corruption	Source assessment, EDD, management decision and reporting where required

Schedule 2 - Key definitions

Term	Meaning
AML	Anti-money laundering.
Beneficial owner	The natural person who ultimately owns or controls a client or on whose behalf a relationship or transaction is conducted.
CDD	Customer due diligence used to identify and verify a client and understand the relationship.
CTF	Counter-terrorist financing.
EDD	Enhanced due diligence applied to a higher-risk relationship or activity.
PEP	A person entrusted with a prominent public function, together with relevant family members and close associates under the applicable risk framework.
Proliferation financing	Financing connected with proliferation of weapons of mass destruction or related sanctions evasion.
Sanctions	Restrictions imposed by a government or international body on persons, entities, countries, sectors, assets or activity.
Source of funds	The origin of money or assets used for a particular deposit or relationship.
Source of wealth	How a person accumulated overall wealth over time.