NINEVEH
JEWELLERY TRADING

AML / CFT / CPF Compliance Manual

Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing - Official Company Policy

Trade Licence No. 1157535 | Commercial Register No. 1920663 | DCCI No. 448123 | Effective Date: 30 July 2026

1. Purpose

This Manual sets out how Nineveh Jewellery Trading Co. L.L.C ("the Company") identifies, assesses, and manages money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risk in the course of its business as a trader in jewellery, precious metals, and gemstones, including gold, and reaffirms the Company's commitment to avoiding association with serious human rights abuses, conflict, and environmental degradation in its supply chain.

2. Scope

This Manual applies to all owners, managers, employees, and representatives of the Company, and to all business relationships and transactions, including onboarding of clients, suppliers, and other counterparties.

3. Legal and Regulatory Framework

On a national level, this Manual is based on, and must be read together with:

- Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, Proliferation Financing, and Illegal Organisations
- Cabinet Resolution No. 134 of 2025 concerning the Executive Regulation of Federal Decree-Law No. 10 of 2025, including the AED 55,000 cash-transaction threshold for DPMS set out in Article 3(3)
- Ministry of Economy and Tourism (MoET) Supplemental Guidance for Dealers in Precious Metals and Stones and related circulars

On an international level, the Company has regard to the FATF 40 Recommendations and 11 Immediate Outcomes, the standards of the Middle East and North Africa Financial Action Task Force (MENAFATF), and the UN Global Programme against Money Laundering (GPML).

4. Governance

The Company has designated the Director and the Compliance Officer as its AML Policy compliance persons, with joint responsibility for the enforcement of this Manual. Together they are ultimately responsible for compliance with all relevant laws, regulations, rules, and professional standards applicable to the Company with respect to AML/CFT/CPF, for ensuring the Company keeps and maintains all required AML records, and for ensuring relevant reports are filed with the UAE authorities when appropriate.

4.1 Director

Anton Bit Killeta acts as Director for the purposes of this Manual. The Director's roles and responsibilities are:

- Approve an effective framework, including internal policies, controls, and procedures, to mitigate the identified risks
- Approve business relationships with high-risk customers
- Constantly screen and monitor events and incoming legislation to identify new requirements, threats, and risks, and opportunities to address these
- Review, scrutinise, and study records and data concerning Suspicious Transactions, and decide whether to notify the FIU or maintain the relationship, with reasons, while maintaining complete confidentiality
- Review and comment on the semi-annual reports of the Compliance Officer
- Upon request of the Central Bank of the UAE, disclose the requested information and documents for examination and verification
- Report to and cooperate with supervisory authorities and the FIU, and allow their authorised employees to view necessary records and documents

4.2 Compliance Officer

Denis Arkhipov (da@nineveh.ae, +971 58 548 6219) acts as Compliance Officer for the purposes of this Manual. The Compliance Officer's roles and responsibilities are:

- Develop an effective framework, including internal policies, controls, and procedures, to mitigate the identified risks
- Regularly review and update internal rules and procedures relating to combating money laundering, assess their consistency with UAE legislation, and assess the Company's adherence to them
- Prepare semi-annual reports covering the above review to the Director, who forwards a copy to the relevant supervisory authority together with the Director's remarks and decisions
- Perform a risk assessment on the Company's overall activities, including contemplated activities
- Carry out individualised customer due diligence
- Perform onboarding and identity verification processes
- Detect transactions relating to any money laundering crime
- Constantly screen and monitor events and incoming legislation to identify new requirements, threats, and risks
- Upon request of the Central Bank of the UAE, disclose the requested information and documents for examination and verification
- Report to and cooperate with supervisory authorities and the FIU, filing DPMSR/STRs via goAML and maintaining the Company's goAML registration

4.3 Staff conduct and acknowledgment

Staff are expected to act in a manner that reaffirms and enhances the Company's reputation for honesty, integrity, and reliability. Adherence to this Manual is a condition of employment or engagement. Staff must acknowledge on an annual basis that they have understood this Manual and have disclosed any suspected or actual violations through appropriate channels.

4.4 Training

The Company arranges regular AML/CFT/CPF training for all relevant employees, covering ML/TF/PF risks, mitigation measures, customer due diligence, identifying red flags, and reporting suspicious transactions. The training programme is documented, and records of sessions, attendance, and content covered are maintained.

5. Risk-Based Approach and Business-Wide Risk Assessment

The Company assesses the ML/TF/PF risks presented by its customers, products, transactions, geographic areas, and delivery channels, to understand what the Company might be exposed to and how it might be affected. The business risk assessment is carried out at least once a year, documented, kept up to date, and made available to the relevant supervisory authorities upon request. It is also reviewed whenever the Company becomes aware of internal or external developments that could affect its accuracy, such as changes in business strategy, new products or markets, or newly identified threats.

For this purpose, the Company maintains an inventory of its suppliers and customers and the products it offers, and defines the scope of business areas to assess. It uses up-to-date quantitative and qualitative information on the types and number of customers, volume of operations by customer type, and volume of business per product and geographic location.

The assessment considers, for each identified inherent risk: its likelihood of occurrence, its timing, and its impact on the Company. The Company classifies identified risks as high, medium, low, or a combination (such as medium-high or medium-low), taking into account the most serious sectoral threats identified in the UAE National Risk Assessment. A risk rated low does not exempt the Company from taking reasonable and proportionate mitigation measures. A summary of the current assessment is at Annex A.

Upon the results of each risk assessment, the Director issues a statement on the Company's risk appetite and the targeted measures to be adopted to prevent or mitigate the identified risks, which is communicated to relevant employees.

6. Customer and Supplier Due Diligence (CDD)

The Company undertakes CDD measures prior to or during the establishment of a business relationship; before executing a transaction for a customer with whom there is no business relationship; before executing any transaction at or above AED 55,000 (whether single or several linked transactions); where there is suspicion of a money-laundering crime; and where there are

doubts about the veracity or adequacy of previously obtained customer data. CDD includes identifying and verifying the customer or beneficial owner, the nature of their activity, the purpose of the relationship, and the ownership and control structure.

Where the crime risk identified is low, the Company may complete verification of the customer's identity after the business relationship has been established, provided verification is completed in a timely manner, the delay does not obstruct the normal course of business, and appropriate measures are applied to control the risk in the meantime.

6.1 Onboarding document checklist

For natural persons, the Company obtains: name as shown on the identification card or travel document, nationality, address, place of birth, and the name and address of the employer, attaching a copy of a valid identification card or travel document, with Director approval if the customer or beneficial owner is a PEP.

For legal persons and legal arrangements, the Company obtains: name, legal form, and Memorandum of Association; headquarters or principal place of business address (and, if the entity is foreign, the name and address of its legal representative in the UAE); articles of association or similar documents approved by the relevant UAE authority; and the names of persons holding senior management positions.

6.2 Reliance exemption

Verification of the identity of a shareholder, partner, or beneficial owner is not required where that information is obtainable from reliable sources and the supplier or controlling owner is a company listed on a regulated stock exchange subject to adequate transparency and disclosure requirements, or a subsidiary whose majority shares are held by the shareholders of such a listed holding company.

7. Beneficial Ownership Identification

For corporate counterparties, the Company identifies and verifies the natural person(s) who, individually or jointly, hold a controlling ownership interest of 25% or more in the legal entity. Where no individual can be identified on this basis, the Company identifies the individual(s) holding senior management positions within that entity. Once beneficial owners are identified, the Company performs CDD on each individual beneficial owner. This is subject to the reliance exemption at 6.2 above, and is refreshed periodically and upon any known change.

8. Enhanced Due Diligence (EDD) and Politically Exposed Persons (PEPs)

For the purposes of this Manual, a Politically Exposed Person (PEP) means: a natural person who is or has been entrusted with a prominent public function in the UAE (a domestic PEP) or in any other country (a foreign PEP), such as a head of state or government, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation, or senior official of a political party, and persons entrusted with the management of, or a prominent function within,

an international organisation; direct family members of a PEP (spouse, children, spouses of children, and parents); and known close associates of a PEP, including persons with joint or sole beneficial ownership of a legal person or arrangement established for the benefit of a PEP.

For foreign PEPs and their related persons, the Company will: determine whether a customer or beneficial owner is a PEP, a direct family member, or a known close associate; obtain Director approval before establishing, or continuing, a business relationship; take reasonable measures to establish the source of funds and wealth; and conduct enhanced ongoing monitoring of the relationship.

For domestic PEPs and heads of international organisations and their related persons, the Company will take sufficient measures to identify whether the customer or beneficial owner is such a person, and will apply the same source-of-funds and enhanced-monitoring measures only where the relationship is otherwise assessed as high-risk.

More generally, EDD is applied to high-risk customers and legal entities with complex ownership structures, and includes: obtaining and investigating more information relating to the customer's or beneficial owner's identity or the purpose of the relationship; updating CDD information more systematically; taking reasonable measures to identify source of funds; obtaining information on anticipated transaction size, turnover, counterparties, and locations of activity; and obtaining senior management (Director) approval to commence the relationship.

9. Risk Categorisation

Each counterparty is categorised as low, medium, or high risk based on factors including: country/jurisdiction of the counterparty and of the underlying goods; nature of the business relationship and transaction; whether the counterparty or a related party is a PEP; and sanctions screening results. See Annex A for the full set of risk factors used.

10. Sanctions and Targeted Financial Sanctions (TFS) Screening

During onboarding and on an ongoing basis, the Company screens potential and current customers and counterparties to ensure they do not appear on the UN Consolidated List, the UAE Local Terrorist List, the GCC countries terrorist list, the US OFAC Specially Designated Nationals and Blocked Persons list, and other lists administered under UAE law. As these lists are updated frequently, the Company consults them regularly and subscribes to receive updates when they occur. The Company will not engage in a business relationship, or a transaction, with a party on a sanctions list or prohibited by UN or UAE economic sanctions and embargoes, and will report any such encounter. Any match is escalated to the Compliance Officer and the Director for investigation and appropriate action.

11. Cash Transaction Threshold and DPMSR Reporting

Any single cash transaction, or several linked cash transactions, equal to or exceeding AED 55,000 is reported to the UAE Financial Intelligence Unit as a Dealers in Precious Metals and Stones Report

(DPMSR) via the goAML platform, regardless of whether the transaction is suspicious. This includes cash instalment or advance payments and unfixed gold transactions in cash meeting the threshold. For such transactions, a copy of the customer's identification documents (or, for legal entities, the trade licence and the identification of the representing person) is registered in goAML.

12. Cash Acceptance Procedures

The Company will always make and receive payments for gold through official banking channels wherever possible, ensuring that payment methods and financial instruments used are consistent with the customer's profile and do not disguise the origin of funds. The Company will not deal with shell banks (banks with no physical presence in their country of incorporation and licensing that are unaffiliated with a regulated financial group subject to effective consolidated supervision), including by accepting funds from them.

Where payment through official banking channels is not possible and a cash transaction is unavoidable, the Company may engage in one, subject to conditions. Before accepting cash, the Company verifies the origin and legitimacy of the customer's cash, regardless of the amount involved. Where a cash transaction proceeds, employees record as much information as possible, including the denomination of banknotes, banknote serial numbers where possible, and documents corroborating the customer's source of funds. Where a cash transaction involves a third party acting on the customer's behalf, the Company obtains and retains documentation authorising that representation. Any significant discrepancies or red flags identified during the cash acceptance process are escalated to the Director and Compliance Officer for investigation, and reported to the supervisory authorities if necessary.

13. Suspicious Transaction Reporting (STR)

Where Company employees have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute or relate to the proceeds of a money-laundering crime, or are intended for use in such activity, regardless of amount, they must, without invoking professional or contractual secrecy: file a Suspicious Transaction Report with the UAE Financial Intelligence Unit without delay via the goAML platform, and respond to any further information requested by the FIU. Employees maintain confidentiality with regard to both the information reported and the fact of reporting, and must not disclose to a customer or any other person that a report has been made, is being made, or that an investigation is underway ('tipping off'). Employees are not legally liable for administrative, civil, or criminal liability for reporting in good faith. Failure to report a suspicious transaction, whether intentionally or through gross negligence, is a federal offence carrying significant administrative fines and potential imprisonment.

14. Whistleblowing and Internal Reporting

Staff may report concerns about suspicious activity, sanctions matches, or non-compliance with this Manual - including concerns about colleagues or management - directly to the Compliance Officer. Reports made in good faith are treated confidentially, and the Company will not penalise or

retaliate against a staff member for making one. Where a concern relates to the Compliance Officer or Director personally, it may be raised directly with the shareholders.

15. Record Keeping and Data Security

All records, documents, data, and statistics for local and international commercial and cash transactions are kept on a computerised database for a minimum of five (5) years from the date of completion of the transaction or termination of the business relationship, or, where applicable, from the date of completion of a supervisory inspection or the date of a final judgment of the competent judicial authorities. Records are protected from unauthorised access and organised to permit data analysis and tracking of financial transactions, and are made available immediately to relevant authorities upon request. Personal information is stored and processed securely and protected against unauthorised or unlawful processing, loss, theft, destruction, or damage.

16. Independent Audit

The Company engages an independent auditor to conduct periodic audits of its AML/CFT/CPF framework to assess its effectiveness and compliance with regulatory requirements and to identify areas for improvement. The audit covers the Company's policies, procedures, risk assessment, training programme, and record-keeping practices. Audit findings and recommendations are documented and reported to the Director and Compliance Officer for information and any necessary remedial action.

17. Policy Review

This Manual is reviewed at least annually, and whenever there is a material change in applicable law or in the Company's business or risk profile.

Annex A - Business-Wide Risk Assessment

Risk category	Key factors	Indicative rating
Counterparty risk	Mix of corporate and individual counterparties; supply-chain participants; PEP exposure assessed at onboarding	Medium
Geographic risk	UAE domestic activity plus cross-border sourcing/counterparties, including higher-risk jurisdictions and CAHRA exposure	Medium-High
Transaction risk	Mix of cash and bank-settled transactions; volumes and concentrations reviewed against prior shipments	Medium
Product risk	Gold, precious metals, and gemstones - high intrinsic value, portable, and, where recyclable/scrap, harder to trace to origin	Medium-High
Delivery-channel risk	Predominantly face-to-face onboarding; physical delivery and third-party transport used for some shipments	Medium

A.1 Counterparty Risk Factors

The Company analyses the following information collected from the counterparty:

KYC information of suppliers, including information about the origin and transportation of the gold
Identified red flags in the supply chain
Number of participants in the supply chain
Extent and effectiveness of the counterparty's own due diligence practices
Counterparty's conformance with OECD Guidance when sourcing gold
Whether the counterparty's due diligence practices have been audited by a qualified third-party auditor
Length of establishment of the supplier or other counterparty in the supply chain
Complexity of the counterparty's ownership structure, including multiple layers of ownership or use of trusts/similar vehicles apparently for anonymity
Size of the supplier's mining operations (artisanal/small-scale, ASM, or large-scale, LSM), if applicable
Involvement of any PEPs
Adverse media or sanctions findings through screening of suppliers and other supply-chain actors

A.2 Geographical Risk Factors

The Company uses reasonable efforts and recognised sources to identify the location and origin of gold sourced, considering at minimum:

The AML/CFT regulatory environment in the supplier's jurisdiction
Level of conflicts or human rights abuses in any location comprising part of the supply chain
Level of bribery and corruption in that location
Level of involvement, or potential involvement, of criminal organisations
Access from that location to nearby markets or processing operations termed Conflict-Affected and High-Risk Areas (CAHRA)
Level of enforcement of laws addressing significant criminal activity
Payment mechanism used (formal banking system vs. non-banking system)
Existence of international sanctions or embargoes directed at the country or persons within it
Involvement of countries identified as CAHRA

A.3 Transaction Risk Factors

Counterparties and their transactions are screened for:

Inconsistency of the transaction with local or market practices (amount, quality, potential profit, etc.)
Inconsistency of volumes, types, and concentrations of material compared with previous shipments from the same counterparty
Use of excessive cash in transactions
Attempted structuring of transactions to avoid government thresholds
Probability of adverse impacts of the transaction
Gold transported that cannot reasonably be reconciled with its declared location of origin, or an unexplained geographic distance in the supply chain

A.4 Product Risk Factors

The nature of the gold supplied - ASM or LSM gold, gold by-product, melted recyclable gold, or unprocessed recyclable gold - noting risk varies by product type
Level of concentration of gold in the supplied material

A.5 Delivery Channel Risk Factors

Physical delivery of gold to unrelated third parties inconsistent with normal business practice
Courier/transport-related risk factors, including physical security practices such as sealed security boxes, and the likelihood of tampering or content removal in transit
Extent of reliability and KYC information of third-party transportation companies, validated through accepted standards

Adoption and Certification

This AML / CFT / CPF Compliance Manual is adopted as an official policy of Nineveh Jewellery Trading Co. L.L.C ("the Company") by resolution of its shareholders, effective from the date stated above. This document may be provided to banks, business partners, and regulatory authorities upon request as evidence of the Company's compliance framework.

Effective date: 30 July 2026

Review cycle: Annually, or earlier if regulatory requirements change

Approved by:

Anton Bit Killeta

Director, Nineveh Jewellery Trading Co. L.L.C

Date: 30.07.2026

نينوه لتجارة المجوهرات ومصوغات الذهب والفضة
شركة الشخص الواحد ذ.م.م
NINEVEH JEWELLERY TRADING CO. L.L.C
Dubai - U.A.E.

Prepared and administered by:

Denis Arkhipov

Compliance Officer, Nineveh Jewellery Trading Co. L.L.C

Email: da@nineveh.ae | Phone: +971 58 548 6219

Date: 30.07.2026

Company stamp: