Compliance Team

ANTI-MONEY LAUNDERING & COUNTERING FINANCING OF TERRORISM

2023-2024

POLICY STATEMENT:

Aureus Enterprises DMCC is a licensed entity established in United Arab Emirates having License Number "DMCC- 545639" since 24th October 2018 with registered office at Unit.No.AU-32-H,Gold Tower (AU), Plot No: JLT-PH1-13A, Jumeirah Lake Towers, Dubai, UAE operating name as "Aureus Enterprises DMCC" is supervised by Ministry of Economy as its reporting entity and is committed to prevent Money Laundering and Countering the Financing of Terrorism and Proliferation Financing Risk in any manner while operating its business.

Aureus Enterprises DMCC, as a business entity and trade license holder conducts following business in the UAE recognized as Dealers in precious Metals & Stones also known to have its activities categorized under Designated Non-Financial Businesses & Profession "DNFBP's" by its supervisory authorities.

1. Non- Manufactured Precious Metals Trading
2. Imitation Jewellery Trading
3. Jewellery Trading
4. Watches & Clocks & Spare Parts Trading

The management understands the importance of application of the standards and guidelines issued by Ministry of Economy and the supplementary guidance for industry best practices while doing the transactions and conducting businesses in the UAE. The company provides its services and products to local & International markets and implements stringent compliance regime across its operations. The company has conducted internal risk assessment based on Risk based approach including the FATF Standards by considering country risk, customer risk, products, services & transaction risk & delivery channel risk including other attributes and has adopted appropriate risk classifications, it has further considered the outcomes and guidelines of UAE's NRA (National Risk Assessment) & Typologies including sectorial risks and its guidelines.

The company engages in following ethical practices with adherence to sourcing its raw materials from its local as well as international vendors and ensures it conducts all its transactions local and cross border in a manner to adhere with all applicable home and host regulations on AML/CFT& PF including all applicable rules, laws & regulations. The Company deals with miners , refineries, other precious metal dealers within the industries, banks and license export houses also known as agents and retailers & wholesalers ,but mainly it has customers who are business owners and transactions are mainly B2B as it conducts trading in souring gold, silver , precious metals, and at times into pearls & precious stones, however the focus has always been and mainly engaged in trading of gold & silver bars, bullion and precious metals for Business to business clients and gold refineries in the UAE, majorly into sourcing of gold asper the UAE laws and Regulations on AML/CFT following the federal decree law no.20 of 2018 and the cabinet decision no.(10) of 2019 on the executive regulation of federal decree-law no.20 of 2018 and its amendments. It covers important markets related to its sector of product lines and has conducted risk assessment and due diligence process with regards to the type of clients and sourcing parties involved like licensed vendors , licensed agents and licensed refineries and applied suitable internal controls to manage its risks in an effective manner, it applies Simplified Due Diligence for low risk customers and standard due diligence for medium risk customers and EDD (Enhanced Due Diligence) for all High risk customers, all intermediaries involved in the supply chain and customers from jurisdictions considered as high risk based on FATF country list and know your country list , further in the policy & procedures a detailed references are provided.

The management has conducted internal Self Risk Assessment of its business and the type of products and services offered and done an assessment of all its customers and transactions to identify and risk classify its customers and transactions based on jurisdiction, products & services, distribution channels, parties involved in supply chain from souring to refineries , bullion houses involved and all other attributes for identifying the inherent risk and appropriate controls to be applied for deriving the residual risk while operating its overall business.

The Major countries of Interest for sourcing materials & imports for onward exports for trading generally would from below mentioned Countries by applying EDD and suitable controls which are subject to senior management approvals, and especially avoid sourcing from the zones and areas which come under the Conflict-affected and high Risk Areas (CAHRA), The company is currently sourcing/purchasing locally and selling in the UAE including the countries of major business interest are :

India, Ghana, UAE, Peru

The management of Aureus Enterprises DMCC believes that the best way to fulfill this commitment is to establish effective AML/CFT policies, procedures, internal policies, and processes based on Risk Based Approach that are conducive to:

- Carrying out the activities and services provided in accordance with strict ethical standards and current laws and regulations.
- The implementation of codes of conduct and monitoring and reporting systems to prevent that the company is used for money laundering and terrorism financing.
- Ensuring that all the employees of Aureus Enterprises DMCC observe this policy & procedures manual and performs action to the adherence of the processes mentioned in it.

This Policy Manual is:

Reviewed and recommended by:	Approved by:
Compliance Officer/ MLRO	**Shareholder/Board of Directors**

Dated: January 2023

Document Title:	Policy Manual for the Prevention of Money Laundering and Countering the Financing of Terrorism.
Version:	AUEDMCC/AML-CFT/2021/V2.1.02023
Department Belongs to:	Risk and Compliance
Year	January 2023, next Review and Update end of 2023 or any new applicable regulations if any.
Reviewed and recommended by	Compliance Officer
Approved By:	Owners & Board of Directors

Version No.	Date	Sections Changed	Summary of Changes
AUEDMCC/AML-CFT/2020.2.1/V1.0	January 2020-21	Initial Policy and updated with reviewed inputs to be included 2021-22	First Version of Policy with review and recommended changes to include new regulations and sanction screening, TFS, UNSC and UN Consolidate list with monitoring system.
AUEDMCC/AML-CFT/2023/V2.1.02	January 2022-2023, approved in Jan 2023	Updated Policy, with updated regulations and laws	Second version included TFS implementation and relation fines for violations included

TABLE OF CONTENTS

1. BASIS OF POLICY FORMULATION AND REFERENCES

This policy document is based on the guidelines issued by the following regulatory authorities and trade bodies, the document is in adherence with all applicable UAE Laws and Regulations as mentioned herein, the activities of Aureus Enterprises DMCC ultimately is dependent on local Banks & Licensed Financial Institutions (LFI's) for conducting and completing its financial transactions related to the business activities conducted., it's imperative for the company to abide by all laws and regulations related to AML/CFT which directly or due to its relationships with LFI's may have an impact on its trading activities. The below mentioned laws and regulations have been taken into consideration to enhance Aureus Enterprises DMCC's overall AML/CFT Compliance Regime.

- Decree Federal Law No. (20) of 2018 on AML & CFT and Illegal Organizations
- Decree Federal Law No. (26) of 2021 amending certain provisions of Federal Decree Law No. 20 for 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations.
- Cabinet Decision No. (10) of 2019 concerning the implementing regulation of Decree Law No. (20) of 2018.
- Cabinet Decision No. (20) of 2019 regarding terrorism lists regulation and implementation of UNSCRs on the suppression and combating of terrorism, terrorist financing and proliferation of WMD and related resolutions.
- Cabinet Decision No. (74) of 2020 regarding implementation of UNSCRs
- CBUAE Notice No. 74/2019 (19/6/2019) - Procedures on AML/CFT and illegal organizations.
- CBUAE Notice No. 79/2019 (27/6/2019) - Guidelines on AML/CFT and illegal organizations.
- CBUAE Notice No. 103/2020 (24/3/2020) - Regarding UN and Local Lists.
- Federal Law No. (7) of 2014 regarding terrorism offences.
- GoAML Notice - High Risk Country Transaction & Activity Report - 13/04/2021
- Notice No. 3090/2021 - Updated Guidelines on AML / CFT & Illegal Organizations
- Notice No. 3236/2021 - Guidance for LFI's providing services to the Real Estate and **Precious Metals & Stones Sector**
- Notice No. 3895/2021 - Implementation of UN Security Council (UNSC) and UAE Cabinet Resolutions regarding UNSC and Local Lists
- Notice No. 2893/2021 - Guidance on **TFS** & Typologies on the circumvention of **Targeted Sanctions** against Terrorism & Proliferation of Weapons of Mass Destruction
- Notice No. 3556/2021 - Guidelines on AML & Countering Terrorist Financing
- Notice No. 3551/2021 - Guidance for LFI's - Implementation of Targeted Financial Sanctions
- Notice No. 3091/2021 - Guidance for LFI's on Suspicious Transaction Reporting
- Notice No. 4593/2021 - Guidance for LFI's Providing Services to Cash-Intensive Businesses

- Notice No. 4415.2021 - Typologies on AML & CFT in the Financial Sector
- Notice No. 4368.2021 - Guidance for LFI's on Transaction Monitoring & Sanctions Screening
- Notice No. 4711/2021 - AML/CFT & Illegal Organizations Controlled & Dual use Goods for FIs
- Notice No. 5271/2021 - Guidance for Licensed Exchange Houses & Amended Chapters of the Standards for the Regulations
- Applicable Red-flags indicators for suspicious transactions as required by the Article (16) of Cabinet Resolution No (10) of 2019
- Ministry of Economy Guidelines on applying Due Diligence Regulations for Responsible Sourcing of Gold, August 2022.
- Guidance on Targeted Financial Sanction for FIs, DNFBPs and VASPs issued by the EOCN (Executive Office for Control & Non-Proliferation)
- All other relevant laws/regulations and Typology Reports issued by UAE on AML/CFT and international initiatives and best practices, including applicable (Organization for Economic Co-operation and Development) OECD Guidelines for responsible supply chains of mineral from Conflict Affected and High-Risk Areas and its supplements applying to Refiners and other stakeholders in a gold supply chain and therein.

1.1. The Ministry of Economy

The Ministry of Economy is fully committed to countering money laundering, combating, detecting, and deterring terrorist financing in accordance with legislation, as the relevant authorities in the UAE have established an institutional system of supervision, control and gathering information on all practices that may lead to and respond to financial crimes, including money laundering and terrorist financing. The authorities are aware that the national framework and coordination to address money laundering and combat terrorist financing must continue to be strengthened and developed to improve its effectiveness.

As a reporting entity for Designated Non-Financial Businesses and Professions (DNFPB) expects:

- Strict compliance with applicable Anti-Money Laundering and Terrorism Financing Laws - Decree 20 of the Federal Law 2018 on countering money laundering offences, combating terrorist financing and financing illegal organizations and
- As well as with the recommendations and circulars issued on this subject - Regulations 10 of 2019 for a decree of federal law No. 20 of 2018 on countering money laundering crimes, combating terrorist financing, and financing illegal organizations
- Cabinet Decision No. (20) of 2019 Terrorism List Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing and proliferation of Weapons of Mass Destruction, and Related Resolutions.
- Cabinet Resolution No. (16) of 2021 on the Consolidated List of Offences and Administrative Fines
- Cabinet Resolution No. (53) for 2021 on administrative sanctions resulting from violators of the provisions of The Council of Ministers Resolution No. (58) for 2020
- Cabinet Resolution No. (58) for 2020 on regulating the actions of the real beneficiary
- Cabinet Resolution No. (74) of 2020 on the system of lists of terrorism and the implementation of Security Council resolutions on the prevention, suppression and financing of terrorism, cessation of arms proliferation and financing and relevant resolutions

- Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organization's (the "AML-CFT Decision")
- Strict compliance with Due Diligence Regulations for Responsible Sourcing of Gold, August 2022 and its applicability to adopt and commit to a policy for Gold Supply Chain due diligence and all other guidelines related to Souring, Conduct, Risk Controls, Ongoing Monitoring, Risk Assessment & Management and Reporting Requirements.

Website: www.economy.gov.ae

1.2. The Central Bank of UAE:

The Central Bank of the United Arab Emirates is the state institution responsible for managing the currency, monetary policy, and banking regulation in the United Arab Emirates (UAE).

The Central Bank of the UAE has powers to issue and manage the currency.

- to ensure the stability of the currency.
- to manage the UAE's credit policy.
- to develop and oversee the banking system in the UAE.
- to act as the Government's banker.
- to provide monetary and financial support to the Government.
- to manage the UAE's gold and currency reserves.
- to act as the lender of last resort to banks operating in the UAE; and
- to represent the UAE in international institutions such as the International Monetary Fund, the World Bank, and the Arab Monetary Fund.

The Central Bank of UAE has the following functions: -

- Branches
- Banking Supervision and Examination Department
- Banking Operations Department
- Research and Statistics Department
- Administration Affairs Department
- Financial Control Department
- Treasury Department
- Internal Audit Department

UAE laws on AML/CFT, Frauds, Anti-Bribery and Corruptions

- CBUAE regulation 24/2000 and covers the area of corruption laws.
- Federal Law 4/2002 regarding the Criminalization of Money Laundering.
- Federal Law 9/2014 amending certain provisions of Federal Law 4/2002 concerning the Combating of Money Laundering Crimes.
- Dubai Law 4/2016 on Financial Crimes.
- Cabinet Resolution 38/2014, Executive Resolution of Federal Law 4/2002.
- Federal Law 7/2014, Combating Terrorism Crimes regulations regarding declarations by travelers entering or leaving the United Arab Emirates carrying cash and monetary or financial bearer instruments (issued in 2011).
- Federal Decree Law No 20 of 2018 issued by Ministry of Finance.

- The Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business ("the Standards") Version 1.10 (February 2018)
- National Risk Assessment, issued by National Committee for combating ML/TF (NAMLCFTC) (June 2019)
- Cabinet decision No (10) 2019, issued by Ministry of Finance, (June 2019)

Website: http://cbuae.gov.ae

1.3. United Nations:

United Nations is an intergovernmental organization to promote international co-operation. It was established on 24th of October 1945. At its founding, United Nations had 51 member states. Currently United Nations has 153 members. The headquarters of the United Nations is in Manhattan, New York, USA. The organization is financed by assessed and voluntary contributions from its member states. Its objectives include maintaining international peace and security, promoting human rights, fostering social and economic development, protecting the environment, and providing humanitarian aid in cases of famine, natural disaster, and armed conflict.

The UN has six principal organs:

- the General Assembly (the main deliberative assembly).
- the Security Council (for deciding certain resolutions for peace and security);
- the Economic and Social Council (ECOSOC) (for promoting international economic and social co-operation and development);
- the Secretariat (for providing studies, information, and facilities needed by the UN);
- International Court of Justice (the primary judicial organ); and
- the United Nations Trusteeship Council (inactive since 1994).

UN System agencies include the World Bank Group, the World Health Organization, the World Food Program, UNESCO, and UNICEF.

United Nations Security Council: The Security Council is charged with maintaining and security among countries. While other organs of the United Nations can only make "recommendations" to member states, the Security Council has the power to make binding decisions that member states have agreed to carry out, under the terms of Charter Article 25. The decisions of the Council are known as United Nations Security Council resolutions.

The Security Council is made up of fifteen member states, consisting of five permanent members—China, France, Russia, the United Kingdom, and the United States—and ten non- permanent members. The UN Charter is a multilateral treaty. It is the constitutional document that distributes powers and functions among the various UN organs. It authorizes the Security Council to act on behalf of the members, and to make decisions and recommendations. Resolutions by the Security Council are legally binding if they are made under Chapter VII of the Charter.

Websites:

- http://www.un.org
- http://unscr.com

1.4. Financial Action Task Force (FATF)

The Financial Action Task Force on Money Laundering (FATF) was established in 1989 at G7 Summit in Paris to combat the growing problem of money laundering. The task force was charged with studying money laundering trends, monitoring legislative, financial and law enforcement activities taken at the national and international level, reporting on compliance, and issuing recommendations and standards to combat money laundering.

At the time of its creation, the organization had 16 original members. The FATF Secretariat is housed at the headquarters of the OECD in Paris. In its first year, the FATF issued a report containing forty recommendations to fight money laundering more effectively. These standards were revised in 2003 to reflect evolving patterns and techniques in money laundering. In 2001 the purpose expanded to act on terrorism financing. In February 2012, the FATF codified its recommendations and Interpretive Notes into one document and included new rules on weapons of mass destruction, corruption, and wire transfers.

FATF monitors countries' progress in implementing the FATF Recommendations by 'peer reviews' ('mutual evaluations') of member countries.

Website: http://www.fatf-gafi.org/

2. INTRODUCTION:

Aureus Enterprises DMCC, hereafter may be referred as "Aureus Enterprises DMCC ", Company, Organization, Entity, We, us",

Aureus Enterprises DMCC maintains high standards of professional, social, business ethics and relationship with regulators, customers, peers, developers, and other internal and external stakeholders.

Aureus Enterprises DMCC understands that the business activity of the company is highly Vulnerable to Money Laundering and Terrorist Financing Risks due to the fact that:

Precious Metal (PM) Trading activities represent high intrinsic value in a relatively compact form, tend to maintain (or even increase) value over time, and can be easily transported physically in many forms.

Precious Metal can be used both as means to generate criminal proceeds (i.e., through various predicate offences), as well as vehicles to launder them.

Precious Metal can be used for illicit purposes, including ML/TF, in a variety of ways, either directly (through physical exchange, as a form of currency) or indirectly (through exchange of value via various formal and informal financial systems, as well as via international trade and the financial products and services related to it)

There are large, well-established, decentralized, and often cash-based markets for certain types of precious metals and stones (particularly for gold, but for other PM as well), often allowing them to be traded or exchanged with relative anonymity.

In its relentless efforts to exercise caution in all its transactions, organisation have planned to implement policies and procedures and provide suitable trainings to its staff for the awareness and implementation of guidelines as issued by the Ministry of Economy on AML/CFT.

This internal policy is based on the guidelines issued by the Ministry of Economy for DNFPBs and Supplemental Guidance for Dealers in Precious Metals in the UAE, and other international recommendations and practices by FATF.

3. GOVERNANCE FRAMEWORK:

3.1. Governance Structure for AML/CFT Compliance – Figure 1

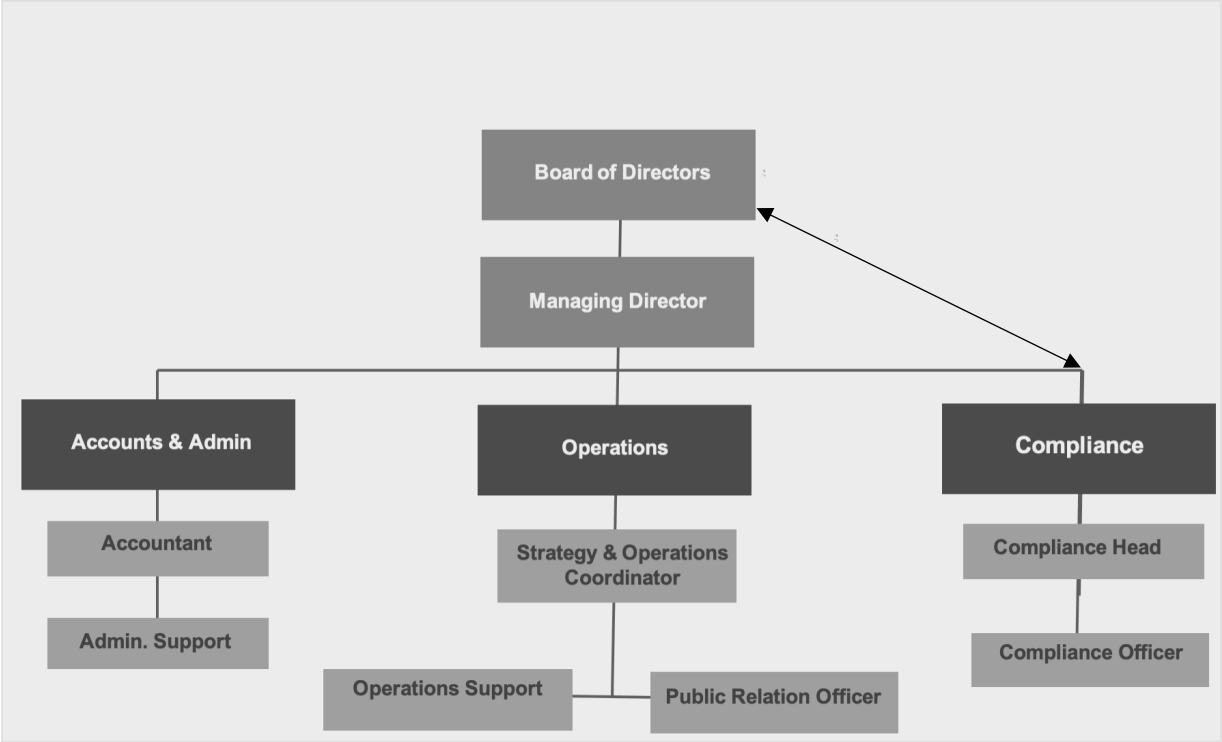


Figure 1: Governance Structure – Aureus Enterprises DMCC, as of January 2023

3.2. Roles and Responsibilities:

3.2.1. Management Roles and Responsibilities: Owner

3.2.1.1. Minimum requirements:

Owners/Board of Directors at Aureus Enterprises DMCC must undertake and govern the compliance activities and functions in Aureus Enterprises DMCC.

Following Functions Shall be undertaken by the Owner:

- Undertake a risk assessment which identifies the vulnerability of the company to be used to launder money or finance terrorists.
- Based on the risk assessment, implement a risk management framework to ensure that the company is not used to launder money or finance terrorists.
- Ensure that the risk management framework is developed, and sufficient resources being devoted to dealing with higher-risk customers and transactions.
- Ensure that the company has appropriate compliance management arrangements, including the appointment of a compliance officer at management level; and
- Devote sufficient resources to deal with money laundering and terrorist financing, including ensuring that the compliance function is adequately resourced, and that staff receive appropriate and adequate training.

3.2.1.2. Actions required.

Owner/Shareholder/BOD (Board of Directors) must:

- Carry out a risk assessment, which should be reviewed and updated on a regular basis, identifying where the business is vulnerable to money laundering and terrorist financing.

- Based on the risk assessment, develop internal policies, procedures, and controls to combat money laundering and the financing of terrorism.
- Ensure staff effectively implements the internal policies, procedures, and controls and receive appropriate training; and
- Monitor the implementation of the company policies, procedures, and controls and make improvements where required on the basis of changes to the company`s money laundering and terrorist financing risk assessment or as recommended by the regulatory authority and/or the financial intelligence unit.

3.2.1.3. Responsibilities

Owner is responsible for the effective implementation of a risk framework of money laundering and terrorist financing risk.

The management of risk needs to be reviewed and updated from time to time to reflect changes in the company`s strategy or other factors such as changes to the law.

Policies and procedures should consider risk factors relating to the customer, product and service, delivery channel, and geographic location of the customer.

Where higher risks are identified, based on the Company`s risk assessment, the staff must take extra measures and senior management should ensure that the staff fully understand and implement the requirements of the policies and procedures.

3.2.2. Management Roles and Responsibilities – Compliance Officer

The Anti Money Laundering Officer is responsible for the following actions:

- Receiving inputs from staff and making suspicious transaction reports to the financial intelligence unit and regulatory authority.
- Developing and maintaining the anti-money laundering and counterterrorist financing policy and internal procedures of the company in line with regulatory requirements.
- Assisting the management in developing and maintaining an effective anti-money laundering and counterterrorist financing compliance culture.
- Ensuring adequate documentation of the Aureus Enterprises DMCC’s risk management policies regarding prevention of money laundering and terrorist financing, risk assessments, and their application.
- Determining and updating, in consultation with the senior management, a risk-based approach regarding money laundering and terrorist financing and the risk assessment of the Aureus Enterprises DMCC’s customers, products, services, delivery channels, and geographic reach.
- Ensuring that all internal suspicious activity reports received are investigated without delay.
- Submitting suspicious transaction reports to the financial intelligence unit (FIU)through goAML System
- Providing initial and updated training for all relevant staff, including all staff who handle transactions, and customer receipts and payments transactions.
- Providing awareness training to the staff and the senior management.
- Ensuring that the staff are aware of and complying with their obligations under the law and the Aureus Enterprises DMCC’s policies and procedures and that the basis for the risk-based approach to managing money laundering and terrorist financing risks is understood and applied.
- Presenting reports to the Board of Directors, making recommendations, if any, for action to remedy any deficiencies in the policies, procedures, systems, or controls and following up on those recommendations.

AML/CFT GUIDELINE AND PROCEDURES:

3.3. Customer Due Diligence Process.

Aureus Enterprises DMCC as dealers in precious metals should carefully consider the following factors while conducting any business relationship with a natural person/Individual, legal entity, or a corporate customer such as;

- Customer Risk:
  Whether the counterparty or customer is a physical person, a legal person, or a legal arrangement, if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a Politically Exposed Person (PEP)—particularly in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level in regard to the product or service and transaction type is appropriate. Politically Exposed Persons are defined by the Financial Action Task Force (FATF) as an individual's who is or has been entrusted with a prominent public

function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing ML/TF offences and related predicate offences, including corruption and bribery. The potential risks associated with PEPs justify the application of enhanced (AML/CFT) preventive measures with respect to business relationships with PEPs.

Further the PEP's can be also classified as Foreign PEPs also known as FPEP's are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials.
Domestic PEP's – DPEP's are individuals who are or have been entrusted with prominent public functions in UAE, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials.
International organizations PEPs – International organization means an entity established by formal political agreements between member countries that have status of international treaties, whose existence is recognized by law in member countries.
Persons who are connected to PEPs, such as the PEPs close relatives or close associates are also classified as PEPs:
Additional Enhance due diligence measures shall be undertaken on customer types identified as PEP's or FPEP's is mentioned under the customer due diligence section.

- Geographic Risk:
  Country of origin of the product, particularly in relation to whether the country is a known production or trading hub for the type of Precious Metals; has adequate regulations and controls ensuring applicable Responsible Due Diligence is identified and applied to avoid non-compliance with OECD and as per UAE Ministry of Economy's guidance on Conflict-affected High Risk Areas (CAHRA) and responsible souring and supply chain due diligence is applied to a High-Risk Country (e.g., is subject to international financial sanctions, has a poor transparency or corruption index, or is a known location for the operation of criminal or terrorist Organization's) and Due Diligence Regulations for Responsible Sourcing of Gold as per UAE Ministry of Economy.

  Country of origin or residence status of the counterparty, intermediaries, refineries, or customer (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country).

- Channel Risk:
  Channel by which the counterparty/customer, parties in a supply chain of Gold or refinery is introduced (e.g., referrals versus walk-in, international versus domestic, in-person or via the internet or other media) and communicates (e.g., remote, or personal contact, direct or indirect through a proxy).

All the above factors to be assessed while onboarding a customer as part of Risk Assessment factors.

Procedure to onboard a Customer:

PEP checks on its customers to include verifying details related to

- Close relatives: these include any individual who is identified to be the PEP's parent, parent-in-law, stepparent, spouse, ex-spouse, children, step-children, adopted children and their spouses, siblings, step-sibling, adopted sibling and their spouses, spouse's siblings and their spouses.
- Close associates include: a natural person who is closely connected to the politically exposed person, either socially or professionally.
- A person who has an account relationship with the PEP and who is not an immediate family member of the PEP.
- A person appointed to advise the PEP in matters of public policy (e.g., political adviser, national security adviser etc.).

- A person in a position to influence a PEP.
- A person who is given the mandate to act on behalf of the PEP.
- A joint beneficial owner of a legal entity or legal arrangement with the PEP, excluding those who are merely providing advisory services in a professional capacity.
- A sole beneficial owner of a legal entity or legal arrangement which is known to have been set up for the benefit of the PEP, excluding those who are merely providing advisory services in a professional capacity.
- Prominent members of the same political party, civil organization, labour or employee union as the PEP.
- Person who is connected with the PEP e.g., through joint membership of a company board.
- For all PEPs and close relatives or associates of PEPs, the compliance team will ascertain the impact of the political connection on the client's Source of Funds, the corruption risk of the country where the PEP held his / her PEP appointment (with reference to the corruption perception index and other adverse media reports), the probability of criminal proceedings and the potential impact on the company's reputation.
- If a customer, or a UBO, is a PEP the company will:
- Classify the PEP as high risk
- Conduct a thorough risk assessment ton the PEP taking into consideration the following for the PEP: Source of Wealth (SO W) & Source of Funds (SOF).
- Obtain the approval of the Client Acceptance Committee to commence or continue the business relationship with the customer.
- Increase the degree and nature of monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.

Following documents to be collected as part of Due Diligence Process:

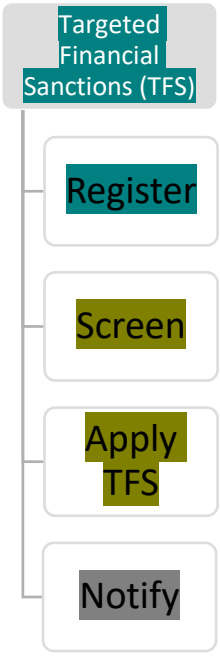
1. KYC Registration Form (Refer Annexure)
2. National ID of an Individual and all Partner/Shareholders/Owners/UBO.
3. Passport copy of an Individual and all Partner/Shareholders/Owners/UBO.
4. Aliases or "aka" names or any other known names for natural/ legal entities to be checked, if any
5. Trade License or Business Registration License Copy with (Online Verification QR code if required)
6. Permanent Residential Address of an Individual and all Partner/Shareholders/Owners/UBO.
7. Tax Certificate if any in case of a Legal Entity.
8. Memorandum of Association / Articles of Association in case of legal entity.
9. Annual Audited Financial Statement to understand business volumes and turnover of the company if the volumes are more than the usual transactions.

3.4. Name Screening & Targeted Financial Sanctions (TFS) & PF Measures:

Aureus Enterprises DMCC is registered for the updates at https://www.uaeiec.gov.ae/ for Local Terrorist List and UN Consolidated list.

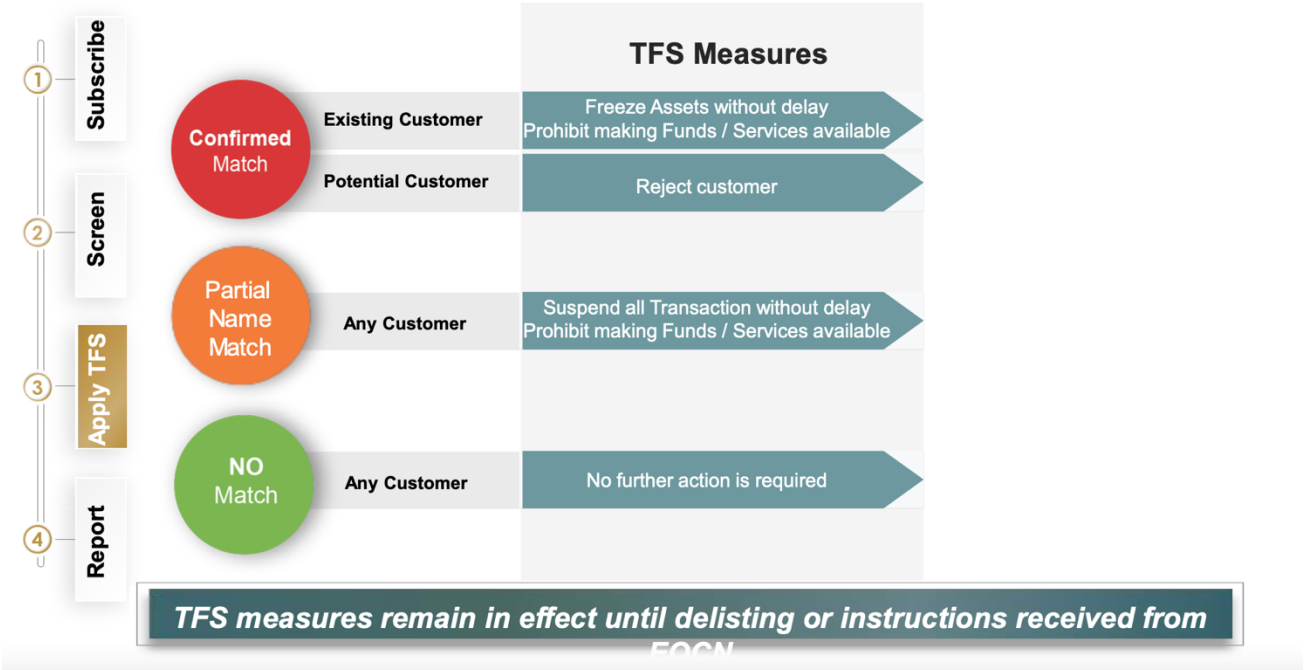
As a DNFBP, Aureus Enterprises DMCC owes a responsibility towards the screening names and addresses against UN Consolidated Sanctions and Local list which is compiled and updated on a regular basis and kept in records for the purposes of identifying designated and prohibited individuals and entities, PEPs and other high-risk entities who may pose a threat to the international community at large. Name screening should be done for all the customers of the organisation and for all the onboarding of the relations and related parties.

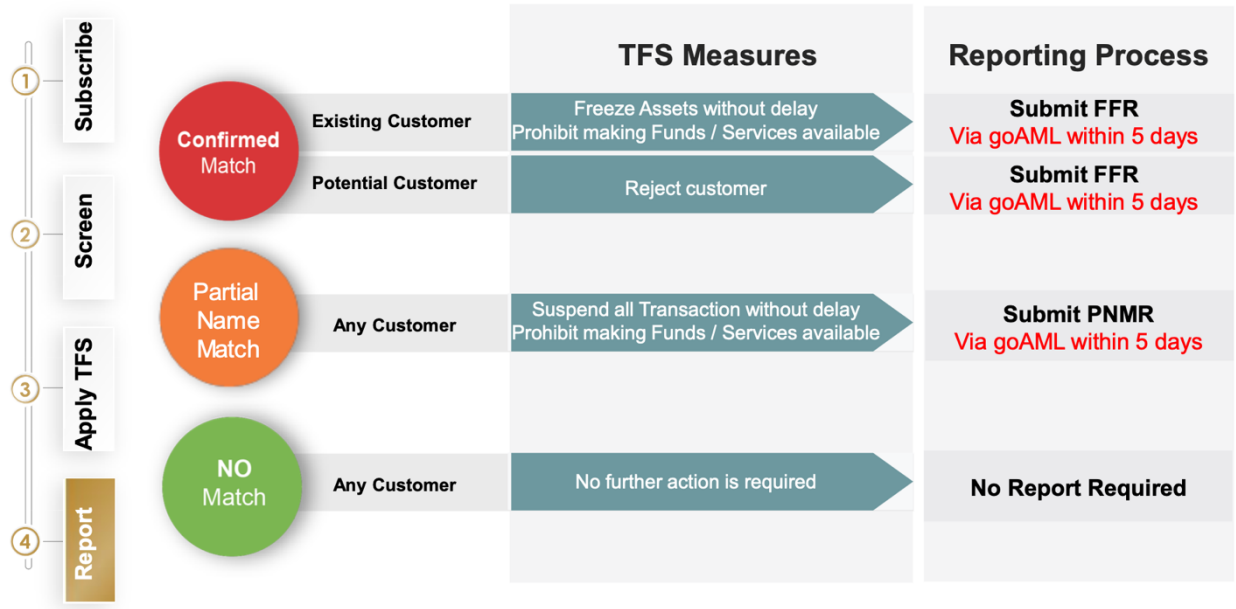
There are four main obligations on all persons, natural or legal in the UAE to implement Targeted Financial Sanctions (TFS)



TFS Implementation Steps

Depending on the type of match, the following TFS measures should apply:





3.4.1. Requirements:

- Aureus Enterprises DMCC should follow the strict adherence to the name screening on each transaction and ensure that no transaction is done with the customer's name that appear in any list (of known specially designated nationals (SDN) or suspected terrorists or terrorist organizations or any blacklist provided by the UAE Regulatory Authorities.
- Aureus Enterprises DMCC ensures that the Name Screening is done on a regular and transactional basis, to check risks related to AML/CFT/PF (Proliferation Financing Risks)
- To check if customers also have any other ownerships or business interests so as to mitigate Risks related to Terrorist Financing, Proliferation Financing Risks and funds or proceeds being used directly or indirectly towards WMD's (weapons of mass destruction)
- Aureus Enterprises DMCC is in process of implementing automatic name screening system which will be integrated with the core system for a real time basis, scans, and filters names of each customer and beneficiary against the sanctioned list, as of date it is screening against the UAE Local list manually.
- In the event that there is a possible match of a customer name with that of the blacklist or UAE local terrorist list, there is a provision to put the transaction on hold manually.
- The details of the name match on the SDN list are checked against details of the customer and beneficiary.
- In the event of an exact match i.e., it is determined that the name is on the blacklist, the transaction is withheld and immediately reported to the Financial Intelligence Unit and the regulatory authority.
- Aureus Enterprises DMCC understand that the failure to report the same could result in fines, penalties, reputational and commercial loss.
- In the event the details of the customer do not match with the SDN list, the transaction and onboarding is released for further processing.
- The blacklists should be updated on a regular basis to avoid omission of names which may be recently added or deleted by the above-mentioned authorities.
- It is recommended to subscribe for alerts from OFAC, UN, EU, and other relevant paid sources.
- Aureus Enterprises DMCC maintains its internal watch list for addition and deletion of the persons with whom the company does not want to deal with according to the risk he/she may expose the company to.
- Any name screening manual process that Identifies as PEP or on sanctioned list is escalated for the approval of the owner with the detailed EDD on the customer once the automated system implementation is completed it will further enhance the procedures.

- The Logs related to the screening of the transactions should be kept for 5 years from the date of transaction for records.

3.5. ISTR (Internal Suspicious Report) and STR/SAR (Suspicious Transaction Report) Procedures:

Internal Suspicious Report is raised internally by the employees to the Compliance Officer to further enable the Compliance Officer and the management to investigate the merits for further reporting the transactions as STR on the goAml system.

As, a primary requirement of submitting Suspicious Transaction Reports (STR), Aureus Enterprises DMCC - has obtained access to goAML, the online STR reporting portal of the Central Bank. The Licensed Person may contact the FIU or the AML Department at Ministry of Economy for appropriate guidance to obtain access to the STR reporting portal.

All employees of the Aureus Enterprises DMCC are obliged personally to report, when there are reasonable grounds to suspect that the funds are proceeds from criminal activity or to be used for money laundering, terrorism or terrorist act or terrorist financing, to the compliance officer. The compliance officer will conduct proper investigations and update the highest authority and raise suitable STR/SAR's. SAR's are generally raised for suspicions surrounding attempted transactions or attempted onboardings by a client or supplier and compliance team has limited details but due the suspicious activity appropriate suspicious activity is raised.

A single Suspicious Transaction Report (STR)/SAR can help stop the flow of illegal money and help prevent the repercussions of financial crime. Further, these reports are an essential contribution to the development of the financial intelligence resources that are used by country's law enforcement, revenue, and national security agencies. Thereby, we file STRs to ensure that the Aureus Enterprises DMCC is not used to aid the transfer of illegal money for money laundering and terrorism financing.

3.5.1. Procedures for iSTR/STR/SAR's:

- All employees are required to report any potentially suspicious or unusual transactions.
- The reporting must be done with full facts of the case within reasonable time.
- It is company`s obligation to investigate the background and purpose of transactions deemed to be 'unusual' and to set forth our findings in writing, even in the event, it is not considered necessary to report the transactions to FIU as suspicious. As is the case of other documents these findings should also be maintained for inspection by the competent authorities for a period of at least five years.
- The Compliance Officer shall conduct in depth investigation and take an appropriate action before reporting such transactions to Financial Intelligence Unit.
- It is important to note that the "time factor" in reporting suspicious transactions remains crucial; if we are able to retrieve / submit the relevant information, it will help regulatory authority and Law enforcement authorities to effectively review and take effective measures to combat money laundering, terrorism financing or any other illegal activity.
- Attempted Transactions are obliged to report transactions through GoAML system, which appear as an attempt to launder money and / or finance a terrorist organization and / or a terrorist activity, Terrorism Financing.

In case of doubt that a transaction might be meant for terrorism or terrorist organizations or for terrorism purposes, we should freeze the transaction / account and inform the financial intelligence unit in writing immediately.
All Employees should strictly comply with the following if a transaction created at your end / found in the system seems suspicious to you:

a. Do not inform the customer of your suspicions about his/her transaction(s), and action being taken by you.
b. Hold the transaction and report immediately to your Compliance Officer.
c. Forward copy of Customer identity and transaction copy to Compliance Officer
d. Hold or block the transaction and do not proceed.

Institutions which fail to report unusual and suspicious transactions shall be penalized in accordance with the prevailing laws and regulations, such incidents should be immediately reported to the authorities through the proper systems.

3.5.2. Tipping Off:

All suspicious transactions must be kept fully confidential, and no one should inform any person or customer that his/her transaction is being reported as a suspicious transaction to the FIU.

Non-compliance is a criminal offence, and the employee involved shall be terminated, immediately and additionally he/she is personally subject to a fine or imprisonment or both.

It is a criminal offence for an employee to tip off, tell or inform any person including customers that any of their transactions is being scrutinized for possible involvement in suspicious money laundering operations or terrorist financing.

Unless there is a FFR after reporting to the authorities and on receiving confirmation from the EOCN the compliance officer can inform the customer to approach EOCN for getting appropriate clearance applications for unfreezing possibilities.

3.6. Red Flags, Unusual, Suspicious Customer and Transactions

The company has a documented list of **red-flags indicators** for suspicious transaction as required by Article (16) of Cabinet Resolution No. (10) of 2019.

Few key indicators of suspicious Customers and Transactions are: -

3.6.1. The Business Relationship, Counterparty, or Customer:

- Suddenly cancels the transaction when asked for identification or information.
- Is reluctant or refuses to provide personal information, or the DPMS has reasonable doubt that the provided information is correct or sufficient.
- Is reluctant, unable, or refuses to explain:
    - their business activities and corporate history.
    - the identity of the beneficial owner.
    - their source of wealth/funds.
    - why they are conducting their activities in a certain manner.
    - who are they transacting with?
    - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.
- Is a designated person or organisation (i.e. is on a Sanctions List, EOCN-TFS/UNSCR List).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
- Actively avoids personal contact without sufficient justification.
- Is a politically exposed person or has familial or professional associations with a person who is politically exposed.
- Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for doing business with the DPMS.
- Is located a significant geographic distance away from the DPMS, with no logical rationale.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction, or is unfamiliar with the details of the requested transaction.
- Makes unusual requests (including those related to secrecy) of the DPMS or its employees.
- Is prepared to pay substantially higher fees than usual, without legitimate reason.

- Appears very concerned about or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Requests services (for example, smelting and reshaping of gold into ordinary-looking items) that could improperly disguise the nature of the PM or conceal beneficial ownership from competent authorities, without any clear legitimate purpose.
- Claims to be a legitimate DPMS but cannot demonstrate a history or provide evidence of real activity.
- Is a business that cannot be found on the internet or social business network platforms (such as LinkedIn or others)
- Is registered under a name that does not indicate that activity of the company is related to PMS, or that indicates activities different from those it claims to perform.
- Is a business that uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have Authorized the transaction.
- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering, terrorism financing, or corruption risk.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense.
- Appears to be acting according to instructions of unknown or inappropriate person(s).
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for short-cuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Request's payment arrangements that appear to be unusually or unnecessarily complex or confusing (for example, unusual deposit or installment arrangements, or payment in several different forms), or which involve third parties.
- Provides identification, records or documentation which appear to be falsified or forged.
- Requires that transactions be affected exclusively or mainly through the use of cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or other such payment methods), or through virtual currencies, for the purpose of preserving their anonymity, without adequate and reasonable explanation.

3.6.2. Transactions:

- Involves the use of a large sum of cash, without an adequate explanation as to its source or purpose.
- Involves the frequent trading of PMS (Precious Metals or Stones) for cash in small incremental amounts.
- Involves the barter or exchange of PMS for other high value metals.
- Appears structured so as to avoid the cash reporting threshold.
- Involves delivery instructions that appear to be unnecessarily complex or confusing, or which involve foreign jurisdictions with no apparent legitimate connection to the counterparty or customer.
- Includes contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Involves payments to/from third parties that do not appear to have a logical connection to the transaction.
- Involves merchandise purchased with cash, which the customer then requests the merchant to sell for him/her on consignment.
- Involves PM with characteristics that are unusual or do not conform to market standards.

- Involves the unexplained use of powers-of-attorney or similar arrangements to transact business on behalf of a third party.
- Appears to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Involves a person acting in the capacity of a director, signatory, or other Authorized representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Involves several successive transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, especially when the nature of the merchandise or the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involves unexplained last-minute changes involving the identity of the parties (e.g., it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the goods, without a logical explanation.
- Involves circumstances in which the parties: – Do not show particular interest in the details of the transaction; – Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms; – Insist on an unusually quick completion, without a reasonable explanation.
- Takes place through intermediaries who are foreign nationals or individuals who are nonresident for tax purposes.
- Involves unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involves indications that the counterparty does not have or does not wish to obtain necessary governmental approvals, filings, licenses, or other official requirements.
- Involves any attempt by a physical person or the controlling persons of a legal entity or legal arrangement to engage in a fraudulent transaction (including but not limited to over- or under-invoicing of goods or services, multiple invoicing of the same goods or services, fraudulent invoicing for non-existent goods or services; over- or under-shipments (e.g., false entries on bills of lading); or multiple trading of the same goods and services).

3.6.3. The Payments:

- Involves cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or similar instruments), negotiable bearer instruments, or virtual currencies, which do not state the true payer, especially where the amount of such instruments is significant in relation to the total value of the transaction, or where the payment instrument is used in a non-standard manner.
- Involves unusual deposits (e.g., use of cash or negotiable instruments, such as traveler's cheques, cashier's cheques, and money orders) in round denominations (to keep below the reporting threshold limit) to pay for PM. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information.
- Is divided into smaller parts or installments with a short interval between them.
- Involves doubts as to the validity of the documents submitted in connection with the transaction.
- Involves third-party payments with no apparent connection or legitimate explanation.

- Cannot be reasonably identified with a legitimate source of funds.

3.7. KYE

Know Your Employee policy should be conducted have the following stages.

a. Pre- Employment Stage
b. Course of employment
c. Employee Conduct

3.7.1. Pre – Employment Stage:

Due diligence in KYE starts at the recruitment stage, to know if the promising candidates are telling the truth.

At the initial stage references should be checked, reference check can be done by the organization or by outsourced agencies.

References of a prospective employee - You can verify if there is any criminal conviction; this can be achieved by getting.

- A police clearance certificate from the police station of the last known residences.
- The relieving letter from the previous employer is taken.
- The past employer can be asked to provide few details like; did they really work for that company stated on the CV? Employment credentials such as designation, role, compensation, conduct and reason for leaving will be ascertained.
- How was their conduct of the prospective employee?
- References provided by the prospective employee can be requested to provide information which the prospective employee has stated on the resume' or job application.
- The references given by the candidate shall be contacted & affirmed. (First degree relations should not be hired)
- In case the verification or background check services are provided by a vendor, Company must ensure the standards & procedures the organization applies while conducting the check. Are their standards comparable to yours? Are there procedures reviewed by an independent firm.
- Screening of Employee names against the sanctions list

3.7.2. Course of Employment:

Even though the reference checks have been applied, it is advisable to have random checks to ensure that the employee maintains its responsibility to be a trustee of the organization. It is good management practice to monitor your employees' performance and understand what makes them stick, but this routine procedure can also unearth internal threats to your business.

3.7.3. Employee Conduct:

Signs which could raise a signal for verifying the employees conduct and behavior: -

- Staff Behavior: A change in the employee's lifestyle, especially when the spending etc. by an employee sees a drastic change then what an employee at the same level could afford.
- Credit cards/Loans: the employees availing frequent loans and credit cards should pose a question for the employer. Too many approvals and NOCs provided to employees can not only lead to defaults but can also cause the organization to be blacklisted for getting further benefits from banks etc.
- Overzealous nature and relation with select customers; There could be possibilities of Customers offering bribes and commissions to employees for conducting frauds, embezzlements and money laundering, Frequent checks, and controls on the activities of employees can help detect these activities at an early stage.
- Timing: Many a times employees employed in critical areas of operations and accounts have been caught for internal frauds etc. These employees have been reported to have long working hours, coming early before the time to office and sitting till late in office.
- Compromising on data & system integrity: employees who have often been reprimanded for misuse of confidential data and systems should be monitored closely for mitigating any risk of fraud.

REGULATORY REPORTING

As a DNFBP and registered Authority Aureus Enterprises DMCC has obligation to report transactions in GoAML System for the following transactions:

3.8. Transactions With Individuals

- All **Cash transactions** with individuals equal or exceeding AED 55,000.00 needs to be reported in the GoAML System.
- Exceptions: (Not to Report) – Any Credit Card /Cheque or Bank Transfer transactions of any amount. Only if Suspicious then to be reported through STR Option in GoAML System.

3.9. Transaction with Legal Entities

- All Cash/ International Wire Transfers / Transfers through Exchange Houses or Remittance Companies equal or exceeding AED 55,000.00 need to be reported in the GoAML System.
- All Settlements in USD with following qualifications.
    - Both Entities having accounts in UAE and transfers done for USD payments.
    - USD Settlements done between two Free zones Within UAE, having different bank accounts, and settlements between Free zone and onshore companies registered in the UAE.

Exceptions: (Not to Report)

- AED Settlement where both the parties have accounts in same bank in the UAE.
- AED Settlement where both the parties have accounts in different banks in the UAE.
- USD Settlement where both the parties have accounts in same bank in the UAE.
- Trade between related parties Mainland to Free zone having same bank account transactions and vice versa.
- Barter transaction (Exchange of Gold)
- Intra Company Transactions
- Transaction not routed through the UAE Bank Account.

INDEPENDENT REVIEW:

A robust AML Compliance program shall be complete where a periodic review to assess the adequacy the policies & procedures, compliance officer's functions and other controls is performed.

The purpose of independent review is to review and test whether the policies, procedures & controls are in line with the regulatory guidelines and to suggest changes and modifications in procedures to have more effective controls in the fight against money laundering and terrorism financing.

3.10. Guidelines:

Both internal & external audits play an important role in evaluating the procedures of Aureus Enterprises DMCC.

a. External Audit: means testing of the internal procedures by an independent party i.e., performed by people not from within the company. The auditors must be sufficiently qualified to ensure that their findings and conclusions are reliable. It is advisable to conduct the independent testing by an external audit firm shall be on an annual basis.

b. Internal Audit: these audits may be performed internally within an organization if there is a provision of an internal audit department or could be outsourced to the efficient partners.
   - There should be a well-defined audit program & checklist.
   - The frequency of such audits may be once in 6 months.
   - The auditor should report directly to the Owner for its findings.

3.11. Scope:

- Examine the adequacy of CDD policies, procedures, and processes, and whether they comply with internal requirements.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers, and geographic locations) on sample testing basis.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Assess compliance with applicable laws and regulations.
- Examine the integrity and accuracy of management information systems used in the AML compliance program if any.
- Reviewing policies, procedures, and processes for suspicious activity monitoring.
- Determining the system effectiveness for reports, blacklist screening, flagging of unusual transactions and more.
- Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transactions. Testing should include a review of policies, procedures, and processes for referring unusual or suspicious activity from all business lines to the personnel or department responsible for evaluating unusual activity.
- Assess the adequacy of recordkeeping.

TRAINING:

The role of AML & CFT training in a dynamic business environment is to be a partner to the employees to help them achieve their objectives. This is achieved by developing the knowledge and skills of the employees. The success of learning, results from its integration with the business plan and the business culture. Hence the prime objectives for Training are:

- To enhance existing knowledge & skills of employees to enable them to successfully accomplish their duties and responsibilities.
- To upgrade the Product Knowledge of Front line / Operations & Sales Staff.
- To adhere to the guidelines of the regulatory authority on employee training.

3.12. Mandatory Teams for Trainings:

3.12.1. New employees – Induction Training

Newly joined employees need to undergo Induction program covering AML/CFT awareness and company`s procedural guide, within fifteen days from joining. This can be conducted internally by the qualified staff from AML/ Compliance Department or through external vendor having expertise in trainings and AML/CFT Knowledge.

3.12.2. Front Line Staff – Induction and Refreshers Training.

All sales staff acts as a first line of defense for AML/CFT program and needs to be trained on an annual basis. These training can be conducted internally by the qualified staff from AML/ Compliance Department or through an external vendor having expertise in trainings and AML/CFT Knowledge.

3.12.3. AML Compliance Department – Continuous Professional Development.

All the employees and members related to AML/Compliance Department shall undergo a Continuous professional development program every year. These trainings can be earned through:

a. AML/CFT conferences or meetings or workshops whether inside or outside the UAE.

b. Face to face training by external agencies whether inside or outside the UAE.
c. Training by industry associations or regulatory bodies; and
d. Web based training

3.12.4. Auditors:

Auditors acts as a third line of defense for AML Program, hence the need to undergo an Awareness and Assessment Training program to audit the operational and AML program implementation of the company. It is advised to conduct an external training program for auditor's minimum once in a year.

3.12.5. Senior Management – AML Awareness Program.

Senior Management and Owners should undergo AML Awareness, Governance and Risk Framework, Latest updates on laws and regulations, minimum once in a year. These trainings shall be organized through the external agencies.

3.13. Topics:

The topics for AML & CTF training should focus on the different levels of employees, i.e., whether the employee is a customer facing employee, a supervisor, or a clerical employee.

The medium and topics of training should be made available as per the nature of the role an employee is working in. The training mediums may be in the form of classroom sessions, circulars, e-learning modules, corridor specific trainings, role plays.

The topics should include:

3.13.1. General information:

Background and history pertaining to money laundering controls, what money laundering and terrorist financing are, why the bad guys do it, and why stopping them is important.

3.13.2. Legal framework:

How the AML Laws apply to institutions and their employees.

3.13.3. Responsibility:

Responsibility of the employees under local laws and regulations for obtaining sufficient evidence of identity, recognizing, and reporting knowledge or suspicion of money laundering and terrorist financing.

3.13.4. Penalties:

For anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment.

3.13.5. Other Topics:

How to react when faced with a suspicious client or transaction & Procedure for reporting of suspicious transactions, how to respond to customers who want to circumvent reporting requirements and Internal policies, such as customer identification and verification procedures and:

- CDD policies.
- What are the legal recordkeeping requirements?
- Red flags.
- Suspicious transaction reporting requirements.
- Duties and accountability of employees.
- Fraud Prevention.
- Tipping off.

RECORD KEEPING:

Records should be kept and made available to Regulatory examiners and for investigation for a minimum of 5 years. The objective for records keeping is to ensure that the company can provide the basic information to reconstruct the transaction undertaken, at the request of the relevant authorities.

3.14. Document retention:

The records prepared and maintained by the company must be such that:

- The requirements of the law and expectations of the regulator or the supervisor are fully met; and Auditors, reporting accountants, and regulators or supervisors are able to assess the effectiveness of Aureus Enterprises DMCC`s AML/CFT policies and procedures.
- Any transaction or instruction conducted through the NBFI on behalf of any individual customer can be reconstructed.
- Any customer or underlying beneficial owner can be properly identified.
- All suspicious transaction reports received internally, and those submitted to the financial intelligence unit, can be identified; and
- The company can meet, within the required time frame, any inquiries or court orders from the appropriate law enforcement agencies.

3.15. How long should records be retained?

- The minimum periods for which records must be maintained to comply with the requirements of the law are outlined in the following table.

Type of Account	Length of Retention
Account opening records and documentary evidence of identity.	At least 5 years after Account Closure.
Account ledger records.	At least 5 years.
Individual transaction records.	At least 5 years.
Results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, usual large transactions).	At least 5 years after Account Closure.
Information after the account has been closed or after the last transaction.	At least 5 years.
AML Training registers.	At least 5 years.

Records relating to a customer's identity must be retained for at least 5 years from the date of closure of business with the client. The date on which the relationship with a customer end is the date of:

- Carrying out a one-off transaction or the last in the series of transactions; or
- Ending of the business relationship, that is, the closing of an account.

FINES AND PENALTIES

As per Federal Decree – Law (20) of 2018.

The Regulator has the authority to impose the following administrative penalties on the financial institutions, designated nonfinancial businesses and professions and non-profit organizations in case they violate the present Decree-Law and its Implementing Regulation:

a) Warning.
b) Fines of no less than AED 50,000 (fifty thousand dirham) and not more than AED 5,000,000 (five million dirham) for each violation.
c) Banning the violator from working in the sector related to the violation for the period determined by the regulatory authority.
d) Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.
e) Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.
f) Arrest or restrict the activity or the profession for a period to be determined by the supervisory authority.
g) Cancel the License.

In all the cases, the Regulatory Authority shall publish the administrative penalties through various means of publication from time to time.

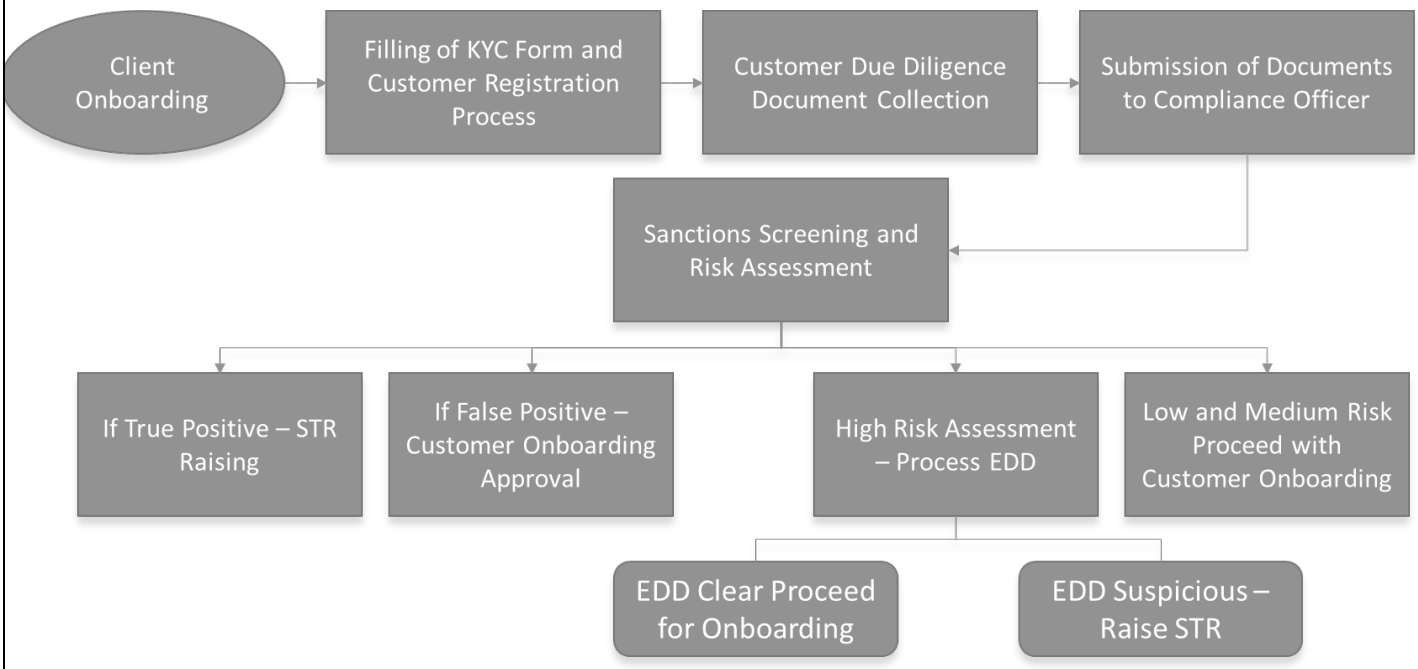
No.	Applicable Article in the Implementing Regulation	Violation	Administrative Fine (AED)
1	Article (4) Clause 1	Failure to undertake the actions and procedures necessary to identify the risks associated with the crime in the violator's field of work.	100,000 AED
2	Article (23)	Failure to identify and assess the risks that may arise in the violator's field of work when developing the services that the violator offers or when conducting new professional practices through its facility.	100,000 AED
3	Article (4) Clause 2	Failure to undertake the actions and procedures necessary to mitigate the risks identified based on the results of the National Risk Assessment or the Self-assessment process given the nature and scale of the violator's business.	50,000 AED
4	Article (20)	Failure to implement internal policies, procedures and controls within the facility aimed at combating crime or preventing involvement in suspicious business relationships.	50,000 AED
5	Article (4) Clause 2/B + Article (22) Clause 1	Failure to take the necessary enhanced due diligence measures to manage high risks.	200,000 AED
6	Article (4) Clause 3	Failure to take the necessary simplified due diligence measures to manage low risks.	50,000 AED
7	Article (5)	Failure to undertake the necessary customer due diligence measures before establishing the business relationship or resuming a business relationship or performing a transaction under the customer's name or in his/her favor.	100,000 AED

8	Article (8) Clause 3	Failure to undertake the necessary measures to understand the purpose of the business relationship and its nature, or the failure to acquire any information pertaining to this purpose when needed.	50,000 AED
9	Article (8) Clause 4	Failure to undertake the necessary measures to understand the nature of the customer's business, the ownership structure of his/her business, and the extent to which the customer has control over that business.	50,000 AED
10	Article (8) Clause 1 and 2	Failure to verify the identity of the customer and the real beneficiary or their representative using documents or data collected from reliable and independent sources before or while establishing a business relationship or opening an account or prior to performing a transaction for a customer with whom no business relationship has been established.	100,000 AED
11	Article (7)	Failure to undertake the due diligence measures pertaining to the ongoing supervision of customers while conducting the business relationship.	50,000 AED
12	Article (13)	Failure to notify the Financial Intelligence Unit of the suspicious transaction report when the customer due diligence measures were not taken before establishing or continuing a business relationship with the customer or performing a transaction for the customer or under his/her name.	200,000 AED
13	Article (17) Clause 1/A	Delay in notifying the Financial Intelligence Unit of the suspicious transaction report in case there is suspicion or if there are reasonable grounds to suspect that the business relationship with the customer is in whole or in part linked to the crime, or that the customer's funds that are subject to the business relationship are in fact proceeds of a crime or were used in committing a crime.	100,000 AED
14	Article (17) Clause 1/A	Failure to provide the Financial Intelligence Unit with the additional information it requires regarding the matter reported in the suspicious transaction report.	200,000 AED
15	Article (14) Clause 1	Dealing with shell banks in any way.	1,000,000 AED
16	Article (14) Clause 2	Opening or maintaining bank accounts using pseudonyms, fictitious names or numbered accounts without the account holder's name.	1,000,000 AED
17	Article (15)	Failure to conduct due diligence measures on politically exposed persons before establishing or continuing a business relationship with such customers.	100,000 AED
18	Article (18) Clause 1	Disclosing, directly or indirectly, to the customer or any other person(s) that they have reported or are intending to report a suspicious transaction.	200,000 AED
19	Article (21)	Failure to appoint a compliance officer	50,000 AED
20	Article (19)	Failure to implement the measures prescribed by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations with respect to customers from high-risk countries.	200,000 AED
21	Article (24) Clause 1	Failure to create records for keeping track of financial transactions with customers.	100,000 AED
22	Article (24) Clause 3	Failure to create records that keep track of financial transactions with the customers in an organized manner, which prevents data analysis and tracking of financial transactions.	50,000 AED

23	Article (24) Clause 2	Failure to keep records and documents related to the financial transaction for a period of five years from the date of concluding the transaction or terminating the business relationship with the customer, or from the date of completion of the inspection of the customers facilities.	50,000 AED
24	Article (24) Clause 4	Failure to make all the information pertaining to the customer due diligence, ongoing supervision, and the results of their analysis, records, files, documents, correspondence and forms available to the competent authorities upon request.	50,000 AED
25	Article (21) Clause 4	Failure to provide training for the facility's employees on combating money laundering and the financing of terrorism.	50,000 AED
26	Article (60)	Failure to take the necessary measures regarding customers included in the international or domestic sanctions lists before establishing or continuing a business relationship with those customers.	1,000,000 AED

ANNEXURE

3.16. Flow Chart - Onboarding of Customer Process



*All Customers are Screened during pre-onboarding stage , during on-boarding stage , during every transaction by the customer, during any changes in customer profile and during any changes in sanctions list.

3.17. Risk Assessment Process for Money Laundering - Individual

Customer	Category 1	Category 2	High Risk	Medium Risk	Low Risk
Individual	Residential Status	Resident Local			
		Resident Expat			
		Non Resident			
	Nationality	Low			
		Medium			
		High			
	Income Status	Salaried - Investment Matching to Profile			
		Salaried - Investment Not Matching to Profile			
		Business - Investment Matching to Profile			
		Business - Investment Not Matching to Profile			
Delivery Channel	Cash	Cash Transaction			
	ATM Deposit	ATM Deposit Transaction			
	Bank Transfer	Bank Transfer from Own Account and Customer Risk is Low			
		Bank Transfer from Own Account and Customer Risk is Medium			
		Bank Transfer from Own Account and Customer Risk is High			
		Bank Transfer from Third Party Account			

3.18. Risk Assessment Process for Money Laundering - Corporate

Customer	Category1	High Risk	Medium Risk	Low Risk
	Main Land Formation			
Corporate	Free Zone Formation			
	Off Shore Company			
	Shell Company	Prohibited		
Partner Nationality	High			
	Medium			
	Low			
Representative Nationality	High			
	Medium			
	Low			
KYC & EDD Documentation	Documentation Complete- ID Proof's			
	Not Complete Documentation- ID Proof's			
	Third Party Documentation			
Delivery Channel	Cash			
	ATM Deposit			
	Managers Cheque			
	Bank Transfer Matching Investment Profile			
	Bank Transfer Not Matching Investment Profile			
	Third Party Transfer			

3.19. List of Country Risk Ratings as on 5th July 2021

Weblink for updating: https://www.knowyourcountry.com/country-ratings-table.

Based upon data collected from many international and government agencies, know your country website has subjectively weighted the findings to provide a free rating tool that is predominantly focused on money laundering and sanctions issues.

Ref: Scoring methodology used by www.knowyourcountry.com , the company will refer to the latest country Risk Rating provided by www.knowyoucountry.com as and when available.

Indicator / Sub Indicator	Weighting
1 Money laundering/terrorist financing risks	52.5
1.1. FATF Uncooperative / AML Deficient	20
1.2. FATF Compliance with 40+9 Rec	15
1.3. US State ML Assessment	7.5
1.4. US Secretary of State terrorism	10
2 International sanctions	15
3 Corruption risks	7.5
4 Global Initiative Criminality Index	10
5 Global Initiative Resilience Index	5
6 EU Tax Blacklist	5

Lower	Lower - Med	Medium	Med - Higher	High

80 - 100	70 - 80	60 - 70	50 - 60	<50

#	Country	Score	Remark
1	Sweden	**87.56**	
2	Åland Islands	**86.64**	
3	Finland	**86.64**	
4	Norway	**86.59**	
5	Svalbard and Mayen	**86.59**	
6	New Zealand	**86.17**	
7	Tokelau	**86.17**	
8	Denmark	**85.92**	
9	Faroe islands	**85.92**	
10	Greenland	**85.92**	
11	Iceland	**85.1**	
12	Estonia	**84.35**	
13	Slovenia	**84.23**	
14	San Marino	**83.91**	
15	Lithuania	**83.51**	
16	Bermuda	**83.4**	
17	Andorra	**82.39**	
18	Namibia	**81.19**	
19	Oman	**80.41**	
20	Vatican City State (Holy See)	**80.24**	
21	Croatia	**80.05**	
22	Austria	**79.97**	
23	American Samoa	**78.84**	
24	Mongolia	**78.11**	
25	South Korea	**77.94**	
26	Macedonia	**77.91**	
27	Germany	**77.82**	
28	Fiji	**77.77**	
29	France	**77.69**	
30	French Guiana	**77.69**	
31	French Polynesia	**77.69**	
32	Guadeloupe	**77.69**	
33	Martinique	**77.69**	
34	Mayotte	**77.69**	
35	New Caledonia	**77.69**	
36	Réunion	**77.69**	
37	Saint Berthélemy	**77.69**	
38	Saint Martin (French part)	**77.69**	

#	Country	Score	Remark
131	Indonesia	**68.49**	
132	Aruba	**68.39**	
133	Cyprus	**68.39**	
134	United Arab Emirates	**68.35**	
135	Malta - on FATF AML Def list	**67.98**	
136	Kiribati	**67.93**	
137	Israel	**67.83**	
138	Kazakhstan	**67.53**	
139	Cote D'Ivoire	**67.46**	
140	Suriname	**67.39**	
141	British Virgin Islands	**67.05**	
142	Sierra Leone	**66.85**	
143	Peru	**66.75**	
144	Angola	**66.74**	
145	Samoa	**66.68**	
146	St Kitts & Nevis	**66.66**	
147	Antigua and Barbuda	**66.57**	
148	Egypt	**66.53**	
149	Malaysia	**66.43**	
150	Sao Tome & Prin.	**66.38**	
151	Palau	**66.3**	
152	Kyrgyzstan	**66.24**	
153	Djibouti	**66.24**	
154	Seychelles	**66.15**	
155	Cape Verde	**65.93**	
156	India	**65.87**	
157	Japan	**65.83**	
158	Montenegro	**65.56**	
159	Dominican Republic	**65.3**	
160	St Vincent & Gren	**65.23**	
161	Tunisia	**65.05**	
162	Curacao	**64.8**	
163	Uzbekistan	**64.8**	
164	Algeria	**64.79**	
165	Serbia	**64.75**	
166	El Salvador	**64.74**	
167	Tajikistan	**64.64**	
174	Mexico	**64.55**	

39	Saint Pierre and Miquelon	**77.69**	
40	Wallis and Futuna	**77.69**	
41	Bhutan	**77.68**	
42	Montserrat	**77.55**	
43	Sri Lanka	**77.34**	
44	Rwanda	**77.09**	
45	Australia	**76.88**	
46	Christmas Island	**76.88**	
47	Cocos (Keeling) Islands	**76.88**	
48	Norfolk Island	**76.88**	
49	Malawi	**76.87**	
50	Ethiopia	**76.87**	
51	United States Virgin Islands	**76.84**	
52	Singapore	**76.83**	
53	Brunei Darussalam	**76.81**	
54	Solomon Islands	**76.76**	
55	Czech Republic	**76.51**	
56	Zambia	**76.5**	
57	Guernsey	**76.44**	
58	Anguilla	**76.16**	
59	Latvia	**76.11**	
60	Chile	**76.09**	
61	Belgium	**76.01**	
62	Switzerland	**75.73**	
63	Greece	**75.61**	
64	Niue	**75.52**	
65	Liechtenstein	**75.42**	
66	Ireland	**75.42**	
67	Qatar	**75.36**	
68	Jersey	**75.34**	
69	Spain	**75.33**	
70	Canada	**75.16**	
71	Saudi Arabia	**75.15**	
72	Mauritania	**75.13**	
73	Isle Of Man	**75.11**	
74	Tonga	**74.96**	
75	Poland	**74.89**	
76	Luxembourg	**74.82**	
77	Puerto Rico	**74.79**	
78	Taiwan	**74.72**	
79	North Mariana Islands	**74.64**	
80	United States	**74.64**	
81	Lesotho	**74.61**	
168	Eritrea	**64.19**	
169	Honduras	**64.15**	
170	Benin	**64.09**	
171	Moldova	**64.09**	
172	Thailand	**64.06**	
173	St Lucia	**63.99**	
175	Belize	**63.89**	
176	Belarus	**63.5**	
177	Mauritius - on FATF AML Def list	**63.47**	
178	Botswana - on FATF AML Def list	**63.4**	
179	Colombia	**63.31**	
180	Vietnam	**63.26**	
181	Armenia	**63.04**	
182	Burkina Faso - on FATF AML Def list	**62.8**	
183	Tanzania	**62.63**	
184	Turkmenistan	**62.49**	
185	Paraguay	**62.25**	
186	Kosovo	**62.07**	
187	Kenya	**61.83**	
188	Nigeria	**61.73**	
189	Azerbaijan	**61.63**	
190	Guinea	**61.62**	
191	Mozambique	**61.02**	
192	Bosnia-Herzegovina	**60.81**	
193	Bahamas	**60.43**	
194	Guatemala	**60.29**	
195	Bolivia	**59.83**	
196	Comoros	**59.52**	
197	Uganda	**59.41**	
198	Mali	**59.22**	
199	Ghana	**59.04**	
200	Lao People's Democratic Republic	**58.94**	
201	Vanuatu	**58.85**	
202	Dominica	**58.78**	
203	China	**58.72**	
204	Ecuador	**58.49**	
205	Trinidad & Tobago	**58.17**	
206	Ukraine	**57.19**	
207	Central African Rep	**56.57**	
208	West Bank (Palestinian Territory, O	**56.44**	

82	British Indian Ocean Territory	74.38	
83	Falkland Islands (Malvinas)	74.38	
84	Pitcairn	74.38	
85	Saint Helena, Ascension and Trista	74.38	
86	United Kingdom	74.38	
87	Slovakia	74.15	
88	Uruguay	74.13	
89	Hungary	74.03	
90	Guam	73.75	
91	Portugal	73.27	
92	Niger	73.26	
93	Marshall Islands	73.24	
94	Micronesia	73.12	
95	Madagascar	73.04	
96	Bulgaria	73.03	
97	Nauru	72.83	
98	Togo	72.78	
99	South Africa	72.71	
100	Nepal	72.66	
101	Cook Islands	72.6	
102	Kuwait	72.57	
103	Italy	72.41	
104	Gabon	72.32	
105	Gibraltar	72.02	
106	Papua New Guinea	71.98	
107	Bonaire, Sint Eustatius and Saba	71.93	
108	Netherlands	71.93	
109	Romania	71.77	
110	Georgia	71.69	
111	Cameroon	71.32	
112	Monaco	71.31	
113	Maldives	71.19	
114	Congo (Brazzaville)	70.6	
115	Bahrain	70.54	
116	Gambia	70.51	
117	Turks & Caicos	70.41	
118	Chad	70.27	
119	Bangladesh	70.13	
120	Equatorial Guinea	70.01	
121	Costa Rica	69.95	
122	Grenada	69.84	
123	Swaziland (Eswatini)	69.78	
124	Hong Kong	69.78	
209	Liberia	56.34	
210	Brazil	56.3	
211	Russian Federation	56.2	
212	Gaza Strip	55.54	
213	Sudan	55.43	
214	Cayman Islands	55.23	
215	Turkey	55.16	
216	Congo, the Democratic Republic	54.81	
217	Burundi	54.64	
218	Cuba	54.28	
219	St Maarten	53.86	
220	Albania	53.61	
221	Cambodia	53.15	
222	Senegal	52.06	
223	Barbados	50.14	
224	Jamaica	49.64	
225	Morocco	48.91	
226	Western Sahara	48.91	
227	Guinea Bissau	47.99	
228	Lebanon	46.08	
229	Venezuela	45.76	
230	Philippines	45.52	
231	Libya	44.62	
232	Pakistan	44.5	
233	Zimbabwe	44.21	
234	Panama	43.84	
235	Iraq	43.71	
236	Somalia	38	
237	Nicaragua	37.65	
238	South Sudan	36.18	
239	Myanmar	36.04	
240	Syria	34.89	
241	Haiti	33.24	
242	Yemen	32.89	
243	Afghanistan	32.1	
244	North Korea	20.93	
245	Iran, Islamic Republic of	17.83	

125	Jordan	**69.54**			
126	Macau	**69.5**			
127	Tuvalu	**69.46**			
128	Argentina	**69.2**			
129	Timor-Leste	**69.13**			
130	Guyana	**68.88**			

KYC (KNOW YOUR CUSTOMER) FORM/KYS/KYBP (KNOW YOUR SUPPLIER/BUSINESS PARTNER OR VENDOR)

Section 1 - General Information - KYC/KYS is mandatory requirement for opening an account with Aureus Enterprises DMCC. The forms are subject to changes/updates as per Regulatory Requirements.

Full Company Name:				
Your Business Address:	Office No.			
	Building Name:			
	Street Address:			
	City:		State:	
	Country:		Pin/Zip/Code/P.O. Box	
Telephone No.				
Fax No.				
Email address:				
Expected Business Volume on Annual Basis				

Section 2 – Ownership Information & Structure

Please state below the details of the owners/partners/managers of the Company.

Full Name:	**Nationality:**	**Contact No.**	**Email Address:**	**PEP (Yes/No), If Yes, please provide details**

Group Company Information

Name of Company:	**Nature of Association & Any other Business Ownerships (%age of shareholding's)**

Section 3 – Regulatory Information

Trade License Details	Issuing Authority		License No.	
	Issue Date		Expiry Date	
Product Registration Details	Reg. No.		Expiry Date	
Commercial Registration Details	Reg. No.		Expiry Date	
Other Registration Status				

Has your business or has any of its Directors, Principals, or Partners been:		
Currently under any legal proceedings or pending judgment in the Court of Law?	Yes☐	No☐
Convicted of or charged with a criminal offense in past 3 years?	Yes☐	No☐
Found liable for negligence, fraud, wrongful trading, or malpractice?	Yes☐	No☐
Subject to any application for, or declaration of, liquidation, bankruptcy, or similar proceedings or subject to an administrative order?	Yes☐	No☐

Refused license or authorization to conduct business has been suspended, withdrawn, or not renewed?	Yes☐	No☐
Censured, fined, disciplined, suspended, or refused membership by any regulatory body?	Yes☐	No☐

Section 4 – Company Legal Information **(please mention details as applicable)**

Company incorporation/Registration Certificate	Date/year of incorporation	☐ PAN No of Co. ☐Trade License No ☐Business Reg Certificate ☐ Cert. of incumbency	Doc No.
	Doc No.		
☐ VAT Registration No. ☐ Tax Reg No ☐ GST Registration No ☐ Other			Valid till
Industry/Association Membership No (Bourse Membership)		Source of funds:	
		Purpose of transaction:	
☐ Company directors / ☐ Share Holder(s) / ☐ Manager / ☐ Authorized Signatory			
Name-		Email-	
Designation-		Mobile No-	
☐ Emirates ID ☐ Director Identification No ☐ Passport No ☐Other Document (Pl. Specify)		Valid Till Date-	

Section 5- Ultimate Beneficial Owner Name/ declaration

*Attach Latest Govt./Authority/Share certificate for UBO(s)-1st level & identity proof			
Name of the Person	Share %	Identity No.(Attach Doc.)	ID Type: Passport/National-ID/Other /Dual Nationality; kindly attach id-copies

Section 6- Bank Details

Bank Name and Address-		Bank Account Number-	
RTGS/SWIFT Code-		IBAN No-	
Account Type/Currency-		Correspondent Bank Name and SWIFT Code	

Section 7- General Information

Does company have and follow AML/CFT Policy?	☐Yes ☐No ☐NA

Responsible precious metal supply chain policy (If dealing in precious metal/jewelry)	
1.Did your company establish a responsible supply chain of gold from conflict-effected and high-risk areas policy which is consistent with the standards set forth in the model supply chain policy in Annex II of the OECD Due Diligence Guidance for responsible Supply Chain of Minerals from Conflict-Affected and High-Risk Areas?	
2.Does your company comply or plan to comply with the OECD Due Diligence Guidance for Responsible Supply Chain of Minerals from Conflict-Affected and High-Risk Areas?	
3.Does the company have a risk-based assessment of its precious metal suppliers/customers? (E.g. Low, medium, high)	

4.Does the company perform enhance due diligence for high-risk precious metal suppliers/customers?	
Is the company complying with any of the following industries initiatives?	
LBMA Responsible Gold or Silver Guidance	
DMCC Risk-Based Due Diligence Guidance for GPM	
RJC Chain of Custody standard	
WGC Conflict Free Gold Standard	
RMI Responsible Gold Standard	
Ministry of Economy - UAE: Due Diligence Compliance with Regulation for Responsible Sourcing of Gold, Precious metals and Stones	

Section 8 - Encl: Documents Attached for above KYC/KYS/KYB

☐ Trade License copy	☐ Company Pan Card copy	☐ Latest Certificate of Incumbency	☐ Business Registration Certificate
☐ VAT Registration Certificate	☐GST Registration Certificate	☐ TAX Registration Certificate	
---Copy of shareholders /Directors/Manager---	☐ Passport	☐ Visa (if applicable)	☐ Emirates ID ☐ Other ID(Pl. specify)
☐ MOA and AOA	☐ Partnership Document (If partnership firm)	☐ Share Certificate	☐ Extract of Company
☐ Certificate of Registration	☐ Certificate of Incorporation		

I/We hereby confirm to the best of my knowledge and belief that the information contained in this form and any attachment hereto is true and correct. I/Wewill timely inform your company in writing of any subsequent material changes to the information provided herein/ attached hereto. Wherein I hereby explicitly agree to abide by all AML/CFT Laws and Regulations of The UAE and shall cooperate further with your company to provide certified true copies including any further information which may be required during the course or after exiting my/our business relationship if requested for the purpose of regulatory reporting's.

Name		Company Stamp
Position		
Signature		
Date		

Additional – COMMENTS if any:

Section 9 - UBO Declaration

Date:
Dear Sir/Madam,

UNDERTAKING LETTER

I , Mr/Ms ....., ... National having Passport number ..... , owner & UBO of (mention company name) hereby confirm that neither of our entities nor any of our related parties are dealing with sanctioned countries as may be listed by UAE, United Nations, United States, European Union or the UK , nor Owned or controlled by , or operating as agents of the Governments of Cuba, Iran, North Korea, Myanmar, Syria or Venezuela or Resident or domiciled in Iran, Syria, North Korea, Cuba or Crimea.

I hereby further confirm that all our business operations have never dealt with / won't involve a sanctioned countries (at present Crimea, Cuba, Iran, North Korea or Syria) or violate or to cause any economic or financial sanctions or trade embargoes implemented, administered or enforced by the United Arab Emirates, The United Nations, United States, European Union, United Kingdom or other relevant sanctions authorities.

I also confirm that neither I nor any of key person acting as nominee of any person national / residing any of the above sanctioned countries.

Thanking you,

For & on Behalf of :_____

SECTION 10 - PEP- Declaration

POLITICALLY EXPOSED PERSON (PEP) DECLARATIONFORM

The information in this form is collected to comply with the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities requirement.

A politically exposed person (PEP) is an individual who is or who has been entrusted with prominent public functions domestically' or by a foreign country.

Prominent public functions include the following profiles:

1. Head of State or of Government

2. Senior politicians

3. Senior government, judicial or military official

4. Member of ruling royal family

5. Senior executive of state-owned corporation / government linked company6. Important political party official

The definition of PEP includes immediate family members, relatives, adviser, close associates, personal adviser or business associate of an individual as set out in FATF's (Financial Action Task Force) Recommendation 12 and 22 and relevant guidance covered under the UAE AML/CFT Laws and Regulations.

1.Are you a PEP? Yes☐ No☐

2. Is you or the entity related to a PEP? Yes☐ No☐
(Please fill the below questions if the first two questions you answered - yes)

3. If you are or related to a PEP, please indicate the profile and relationship to you:

A. Head of State or of Government ☐ B. Senior politician☐ C. Senior government, judicial or military official

☐ D. Member of ruling royal family☐ E. Senior executive of state-owned corporation / Government linked company☐ F. Important political party official☐ G. Other.....

I hereby declare that the details and information given above are complete and true to the best of my knowledge Name:

Designation:

Date & Signature:

Company Stamp

12.ABBREVIATIONS LIST:

Abbreviation	Full form
DNFPB	Designated Non-Financial Business
PM	Precious Metal
ML/TF	Money Laundering/Terrorist Financing
FIU	Financial Intelligence Unit
PEP	Political Exposed Person
UBO	Ultimate Beneficiary Owner
EDD	Enhanced Due Diligence
SAR	Suspicious Activity Report
DPMS	Dealers in Precious Metals and Stones
CDD	Customer Due Diligence
NBFI	Non-Banking Financial Institutions
FATF	Financial Action Task Force
BOD	Board of Directors
NOC	No Objection Certificate
AML Def List	AML Deficiency List

13 FINES AND PENALTIES

As per Federal Decree – Law (20) of 2018

h) Warning
i) Fines of no less than AED 50,000 (fifty thousand dirham) and not more than AED 5,000,000 (five million dirham) for each violation.
j) Banning the violator from working in the sector related to the violation for the period determined by the regulatory authority.
k) Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.
l) Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.
m) Arrest or restrict the activity or the profession for a period to be determined by the supervisory authority
n) Cancel the License.

In all the cases, the Regulatory Authority shall publish the administrative penalties through various means of publication from time to time.