POLICIES AND PROCEDURES MANUAL FOR ANTI-MONEY LAUNDERING AND COMBATTING THE FINANCING OF TERRORISM AND PROLIFERATION FINANCING

AML/CFT/CPF COMPLIANCE POLICY MANUAL

SR BULLION FZCO

Version V 5.0

(16.02.2026)

SR BULLION FZCO

CONTENTS

GLOSSARY OF TERMS USED IN THE AML/CFT/CPF POLICY 5

1. DEFINITION OF MONEY LAUNDERING, FINANCING OF TERRORISM, AND PROLIFERATION FINANCING 7

2. AML/CFT/CPF LEGAL AND REGULATORY FRAMEWORK 9

3. SR BULLION COMMITMENT STATEMENT 12

4. SCOPE OF APPLICATION 13

5. POLICY CUSTODIAN 13

6. PERIODICAL REVIEW 14

7. SR BULLION SERVICES 14

8. GOVERNANCE OF RISK: THREE LINES OF DEFENCE 14

9. POLICY GOVERNANCE 15

10. ROLE OF THE COMPLIANCE OFFICER/MONEY LAUNDERING REPORTING OFFICER 17

11. COMPLIANCE INTERNAL AUDIT 18

12. PURPOSE & RATIONALE 19

13. RISK FACTORS OF SPECIFIC CONCERN TO SR BULLION 19

14. PROCEDURES AND CONTROLS (GENERAL) 22

15. IDENTIFICATION, VERIFICATION AND KNOW YOUR CUSTOMER 22

16. CUSTOMER ONBOARDING 23

17. KYC PROCESS 26

18. RISK-BASED APPROACH 27

19. ENHANCED DUE DILIGENCE 28

20. POLITICALLY EXPOSED PERSONS (PEPS) 29

21. TARGETED FINANCIAL SANCTIONS (TFS) 30

22. UPDATING KYC INFORMATION 31

23. MONITORING OF CLIENT'S ACTIVITIES 31

24. INDICATORS OF SUSPICIOUS ACTIVITIES – RED FLAGS 32

25. REPORTING OF SUSPICIOUS ACTIVITIES 35

26. TYPES OF REPORTING ON GOAML PORTAL 36

27. TIPPING OFF AND CONFIDENTIALITY 37

28. TRAINING AND AWARENESS 37

29. RECORD KEEPING 38

30. RECORD RETENTION POLICY..... 39

SR BULLION FZCO

REVISION RECORD

The Compliance Department of SR Bullion FZCO (hereinafter refereed as ***'SR Bullion'***) will securely maintain the master copy of the document, and they will make periodic updates as required. Any revisions made to the document will be recorded on the Revision Record Sheet provided below:

VERSION	SUMMARY OF REVISION	DATE	DESCRIPTION ON REVISION
V.1.0	First Draft Version	06.06.2023	First Policy Created
V.2.0	Second Draft Version	01.07.2024	Second version of Policy updated in line with recent amendments and circular updates issued by Ministry of Economy.
V.3.0	Third Draft Version	06.03.2025	Policy updated upon appointment of new MLRO (effective February 2025).
V.4.0	Fourth Draft Version	20.05.2025	Policy updated upon change of company name from 'SR Bullion DMCC' to 'SR Bullion FZCO'. (effective 25th April 2025)
V 5.0	Fifth Draft Version	16.02.2026	Fifth version of Policy updated in line with Federal Decree Law No. (10) of 2025 & Cabinet Resolution No. (134) of 2025

SR BULLION FZCO

GLOSSARY OF TERMS USED IN THE AML/CFT/CPF POLICY

AML	Anti-Money Laundering
AMLD	Anti-Money Laundering and Combatting the Financing of Terrorism Supervision Department
CDD	Customer Due Diligence
CFT	Combatting the Financing of Terrorism
CPF	Combatting Proliferation Financing
CBUAE	Central Bank of the UAE
CoP	Code of Practice
DMCC	Dubai Multi Commodities Centre Authority
DNFBPs	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
DPMSR	Dealers in Precious Metals & Stones Report
EDD	Enhanced Due Diligence
EOCN	Executive Office for Control and Non-Proliferation
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FT	Financing Terrorism
ID	Identification
KYC	Know Your Customer
LBMA	London Bullion Market Association
MENAFATF	The Middle East and North Africa Financial Action Task Force
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
NAMLCFTC	National Committee for Combating Money Laundering, the Financing of Terrorism, and Proliferation Financing
Nominal shareholder	A natural or legal person who exercises their associated voting rights in accordance with the nominee's directions and instructions or receives dividends on their behalf. A nominal shareholder is not considered the beneficial owner of any legal entity based on the shares they own as a nominal shareholder.
Nominal manager	A natural or legal person who habitually performs management duties in a company on behalf of the nominee and in accordance with their directions and instructions. A nominal manager of a legal entity is not considered its beneficial owner.

OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PMS	Precious Metals and Stones
RJC	Responsible Jewellery Council
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
VR	Verification
UAE	United Arab Emirates
UBO	Ultimate Beneficial Owner
UN	United Nations

1. DEFINITION OF MONEY LAUNDERING, FINANCING OF TERRORISM, AND PROLIFERATION FINANCING

1.1. The emergence of rapid globalisation and accelerating technological disruption within recent years has caused money laundering, financing of terrorism and proliferation financing to become an issue of unprecedented magnitude. Every day, organisations across the globe see new threats arise due to their global presence and vast diversity of products, services, markets, business lines, and distribution channels. The interconnectedness and integration of the global financial and trade system, ever-changing payment methods, and fewer restrictions on the movement of human capital have given rise to a whole new range of sophisticated methods for criminals to launder money, finance terrorism and facilitate the proliferation of weapons . The need to be more vigilant on an international level has arisen with coordinated and coherent efforts required at various levels to protect the integrity and stability of the international financial system, cut off the resources available to terrorists, and make it more difficult for those engaged in crime to profit from their criminal activities.

1.2. **Money Laundering**

Money laundering is defined as any financial or banking transaction - including its commission through digital systems, virtual assets, or cryptographic technologies - aimed at concealing or changing the identity of illegally obtained funds by passing them through the financial and banking system to make them appear as originating from legitimate sources, and then re-pumping and investing them in a legal manner contrary to their real nature. Simply put, money laundering is the process of making dirty money look clean. Criminals launder money so that they can avoid detection by law enforcement authorities and make personal use of illicit proceeds, including further criminal activity and investment in legitimate businesses.

Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing (the "AML/CFT/CPF Law") defines money laundering as engaging in any of the following acts wilfully, or/and having sufficient indications that the funds are the proceeds of a felony or a misdemeanour including the financing of terrorism, the proliferation financing, and evasion of direct and indirect taxes (i.e., a predicate offence):

- Converts, transfers, or carries out any transaction involving the Proceeds for the purpose of concealing or disguising their illicit origin.
- Conceals or disguises the true nature of the proceeds, source, location, disposition, movement, ownership, or rights related thereto.
- Acquires, possesses, or uses the Proceeds upon receipt thereof.
- Assists the perpetrator of the Predicate Offence in evading punishment therefor.

Stages of Money Laundering:

Despite money laundering being a rather complex series of transactions, which are difficult to separate, it can be simplified into commonly consisting of three primary stages:

1. **Placement**: This is the first stage in separating the illicit funds from their illegal source. During this phase, the initial proceeds that are derived from illegal activities are introduced into the financial system through typically, placing the funds into circulation through formal financial institutions, casinos, the real estate sector, the gold and precious metal industry, restaurant, and other legitimate businesses, both domestic and international.

2. **Layering**: Once the proceeds from the illicit activities have entered the financial system, the next stage in the process involves converting the illegal funds into another form, creating complex layers of financial transactions to conceal the original source and ownership of the funds. This makes it difficult to associate the illegal funds with the predicate crime.
3. **Integration**: This is the third stage that completes the money laundering cycle. By this stage, the laundered funds appear to be legitimate, and it is exceedingly difficult to distinguish between legal and illegal wealth. These integration schemes are done to ensure that laundered proceeds are placed back into the economy in what appear to be normal business or personal transactions.

1.3. **Financing of Terrorism**

The AML/CFT/CPF Law defines Financing of Terrorism as:

Any person who provides, collects, prepares, or obtains funds or other assets, through any means, including digital systems, virtual assets, or encryption technologies, knowing that they will be used wholly or partially in any of the following cases, shall be considered to have committed the crime of financing terrorism:

a) Committing a terrorist act or acts of terrorism;
b) By a terrorist or terrorist organization; or
c) Financing the travel or training of individuals for the purpose of committing, preparing, planning, organizing, participating in, or facilitating a terrorist act.

For this definition, “funds used to finance terrorism” means any money or assets used in full or in part to support terrorism — even if the money comes from a legal source. It does not matter whether the funds were actually used to carry out a terrorist act, or whether they are linked to a specific act. The offence still applies no matter where the person involved is located, where the terrorist group is based, or where the terrorist act takes place.

Financing of Terrorism is also a three-step process of collecting, transmitting, and distributing funds for terrorist activities. This involves raising money, either through illegal or legal channels, and then laundering it through the financial system to conceal its origin and destination. Finally, the laundered funds are distributed to terror cells, who use them to purchase weapons, pay for supplies, or otherwise advance the group's goals. Terrorists regularly adapt how and where they raise and move funds and other assets to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity.

1.4. **Financing the Proliferation of Weapons**

Proliferation Financing refers to the risk of potential breach, non-implementation, or evasion of targeted financial sanctions related to the proliferation of weapons of mass destruction. It involves the risk that funds, financial services, or other economic resources may be used, directly or indirectly, to support the development, acquisition, manufacture, possession, transfer, or use of weapons of mass destruction. This includes attempts to conceal the true purpose of transactions, the identities of the parties involved, or the ultimate destination of goods or funds in order to circumvent international sanctions and export control requirements.

The AML/CFT/CPF Law defines Financing **the Proliferation of Weapons** as:

- The act of providing, collecting, or making available funds or other assets, directly or indirectly, knowing that they will be used, wholly or partially, for the manufacture, acquisition,

possession, development, production, sale, supply, export, transhipment, brokering, transfer, conversion, storage, or use of weapons of mass destruction (WMD), their delivery means, or related materials, including dual-use goods and technologies.

- These activities are considered illegal unless they are specifically allowed under UAE law or under international agreements that the UAE has formally signed. Any actions covered by United Nations Security Council resolutions issued under Chapter VII of the UN Charter—aimed at preventing, stopping, or addressing the proliferation of weapons and their financing—are also treated as criminal offences.

Knowledge and intent may be inferred from factual circumstances in both the crimes of financing terrorism and financing the proliferation of weapons.

2. AML/CFT/CPF LEGAL AND REGULATORY FRAMEWORK

2.1. National Legislative and Regulatory Framework

2.1.1. The UAE is fully committed to combatting money laundering and terrorism financing and detecting deterring them in accordance through established legislation. The competent authorities have put in place an institutional system to oversee, control, and collect information on all practices that may lead to financial crimes, including money laundering and terrorism financing.

2.1.2. Underpinned by its commitment to safeguard the UAE's fiscal landscape from illegal financing and corruption, the National Committee for Combating Money Laundering, the Financing of Terrorism, and Proliferation Financing (NAMLCFTC) was established in 2000 to oversee anti-money laundering policies and efforts in the UAE. Specifically, the Compliance Officer serves to enhance the effectiveness of the AML/CFT/CPF framework in the UAE by ensuring continuous adherence to international standards related to combatting money laundering and terrorist financing crimes.

2.1.3. In August 2020, the Central Bank of the UAE (CBUAE) established a dedicated department, the Anti-Money Laundering and Combatting the Financing of Terrorism Supervision Department (AMLD), to handle all Anti-Money Laundering and Combatting the Financing of Terrorism matters (AML/CFT/CPF). Through AMLD, the CBUAE coordinates closely with the UAE's National AML/CFT/CPF Compliance Officer to implement the National Action Plan effectively.

2.1.4. As a committed member, the UAE contributes to global anti-money laundering efforts and combatting financing of terrorism and proliferation financing(AML/CFT/CPF) and strives to fully implement the standards set by the International Financial Action Task Force (FATF). In 2018, the UAE, with the extensive participation of all concerned authorities, conducted its first national risk assessment on money laundering and terrorist financing, identifying several areas in which the risks are high. The following Laws and their Implementation regulations have been issued to combat the threat of AML/CFT/CPF.

- Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing repealing the Federal Decree Law No. (20) of 2018. .
- Cabinet Resolution No. (134) of 2025 concerning the Executive Regulations of Federal

Decree-Law No. (10) of 2025 concerning Combating Money Laundering Crimes, Combating the Financing of Terrorism and the Financing of the Proliferation of Weapons, repealing Cabinet Decision No. (10) of 2019. .

- Cabinet Decision No. (58) of 2020 Regulating the Beneficial Owner Procedures as amended by Cabinet Decision No. (109) of 2023.
- Cabinet Decision No. (74) Of 2020 On Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combatting of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and ~~its~~ their Financing and Relevant Resolutions.
- Cabinet Resolution No. (71) of 2024 regulating violations and administrative penalties imposed on violators of measures for confronting money laundering and combating terrorist financing subject to the control of the Ministry of Justice and Ministry of Economy & Tourism, repealing Cabinet Resolution No. (16) of 2021.
- Federal Law No. 7 of 2014 on Combatting Terrorism Offences.
- Regulation No. 1/2019 regarding declaration of currencies, negotiable bearer financial instruments, precious metals & precious stones in possession of travellers entering or leaving UAE (issued by the UAE Central Bank on 14/1/2019 pursuant to Article 8 of Federal Law No. 20/2018).
- Federal Decree-Law No. (34) of 2021 On Countering Rumours and Cybercrimes, repealing Federal Law No. 5 of 2012 on Combatting Cyber Crimes.
- Federal Law by Decree No. (31) of 2021 Promulgating the Crimes and Penalties Law, repealing the Federal Penal Law No. 3 of 1987, the Penal Code.
- Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law repealing Federal Penal Procedures Law No. 35/1992, the Penal Procedures Law.
- Central Bank Board of Directors' Decision No. 59/4/219 regarding procedures for AML and CTF and Illicit organisations.
- Guidelines for Financial Institutions on AML/CFT/CPF and illegal organisations issued by the UAE Central Bank on 23/6/2019.
- Ministerial Decision No. (532) of 2019 regarding the establishment of the Anti-Money Laundering Department 2019
- Decision of the Minister of Justice No. 533 of 2019 regarding the procedures for combatting money laundering and financing of terrorism for lawyers, notaries, and professionals.
- Ministerial Decision No. 534/2019 on the establishment of the Compliance Officer for the management of frozen, seized, and confiscated assets.
- Ministerial Decision No. 535/2019 on the procedures for the authorisation application presented by those designated on terrorist lists to use a part of frozen assets.
- Ministerial Decision No. 536/2019 on the mechanism of grievance against the decisions issued regarding listing on local terrorist lists.
- Ministerial Decision No. 563/2019 on the procedures and conditions of the applications for the international judicial cooperation in the distribution of the proceeds of crime.
- Circular No. (2) of 2023 Data Disclosure Notice for Dealers in precious metal and stone.
- Circular No. 1 of 2024 has updated the list of High-Risk Jurisdictions subject to Call for Action and the list of Jurisdictions under Increased Monitoring.
- Cabinet Decision No. (132) of 2023 regarding the administrative penalties imposed on violators.
- Ministerial Decision No. (68) of 2024 Regarding adherence to the Policy of Due Diligence Regulations for Responsible Sourcing of Gold.

- Circular No. (3) of 2024 on updating the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the countermeasures to be applied by Designated Non-Financial Business & Professions (DNFBPs).
- Circular No. (4) of 2024 on updating the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the countermeasures to be applied by Designated Non-Financial Business & Professions (DNFBPs).
- Circular No. (1) of 2025 on updating the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the countermeasures to be applied by Designated Non-Financial Business & Professions (DNFBPs).
- Circular No. (3) of 2025 emphasizing on the importance of screening sanctions and terrorist lists.
- Circular No. (4) of 2025 on Understanding the Importance of the UAE 2024 National Risk Assessment.
- Circular No. (5) of 2025 on Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the countermeasures to be applied by Designated Non-Financial Business & Professions (DNFBPs)
- Circular No. 6 of 2025 on Emphasizing the Implementation of Risk-Based Customer Due Diligence Measures (with a Focus on Simplified Due Diligence)

2.2. International Legislative and Regulatory Framework

2.2.1. Fighting against money laundering, financing of terrorism and proliferation financing is critical for international security, the integrity of the financial system, and sustainable growth. In response to the threats posed by money laundering and terrorist activities, the international community has acted on many fronts, including the creation of various organisations that act as the international standard setters.

2.2.2. The UAE's AML/CFT/CPF legislative and regulatory framework is part of a much larger international AML/CFT/CPF legislative and regulatory framework comprising system of intergovernmental legislative bodies and international and regional regulatory organisations. Based on international treaties and conventions in relation to combatting money laundering, the financing of terrorism, and the prevention and suppression of the proliferation of weapons of mass destruction, intergovernmental legislative bodies create laws at the international level, which participating member countries then transpose into their national counterparts. In parallel, international and regional regulatory organisations develop policies and recommend, assess, and monitor the implementation by participating member countries of international regulatory standards in respect of AML/CFT/CPF.

2.2.3. Among the major intergovernmental legislative bodies, and international and regional regulatory organisations, with which the government and the Competent Authorities of the UAE actively collaborate within the sphere of the international AML/CFT/CPF framework are:

- The United Nations (UN)
- The Financial Action Task Force (FATF)
- The Middle East and North Africa Financial Action Task Force (MENAFATF)

- The Egmont Group of Financial Intelligence Units

3. SR BULLION COMMITMENT STATEMENT

3.1. SR BULLION FZCO ("SR BULLION" or "the Company"), a responsible entity registered with the Dubai Multi Commodities Centre, Dubai, UAE, is committed to supporting both domestic and international efforts to combat money laundering, the financing of terrorism, and proliferation financing. The Company also implements appropriate internal measures necessary to achieve these objectives.

3.2. SR BULLION team considers commitment to uphold strict standards of ethical conduct to be a source to create sustainable value and essential for preserving the stakeholders' confidence. Bearing this in mind, the policies that endorse the strict compliance with the legal framework governing the prevention of money laundering and terrorism financing become a top priority for the Company.

3.3. SR BULLION team is directly responsible for compliance with regulatory standards and assisting in efforts to combat money laundering, financing of terrorism and proliferation financing. The Company wants to convey its position on AML/CFT/CPF via this Policy Document and to reaffirm that the Company will only conduct business activities in strict compliance with all relevant laws, regulations, and best global practices in the domain of AML/CFT/CPF. SR BULLION regards the fight against ML and/or FT or PF as a matter of great importance for the organisation and views it as a collaborative endeavour. SR BULLION's commitment to combatting money laundering and terrorist financing is demonstrated through the publication of this Policy, as well as the implementation and operation of the processes and controls included therein.

3.4. SR BULLION is willing to support and cooperate with:

- Government agencies; and
- Recognised law enforcement agencies, domestic or international,

including global regulatory bodies such as FATF, OFAC, UN, EU, and the local regulatory authority, namely the Central Bank of the UAE (CBUAE) and Anti-Money Laundering and Combatting the Financing of Terrorism Supervision Department (AMLD), as part of any effort in combatting money laundering and/or the financing of terrorism.

3.5. SR BULLION shall maintain the highest operating standards to safeguard the interests of all stakeholders, including customers, shareholders, employees, business partners, and the jurisdiction in which the Company operates. This shall be accomplished through constantly staying updated on international and national AML/CFT/CPF policies, ensuring ongoing and continual training of staff members, usage of up-to-date technology and systems that support the efforts to combat money laundering and counter terrorist financing, and other related financial crimes.

3.6. As an established organisation conducting business in the gold and precious metals sector, SR BULLION is committed to responsibly ensuring that none of its activities and acquisition of materials contributes to Money Laundering, Terrorism Financing, or serious Human Rights abuses, by ensuring that risks associated with gold and precious metals during procurement, distribution, transport, explore and sell and/or purchase, are identified and assessed appropriately.

3.7. As a responsible organisation in the gold and precious metals sector, SR BULLION adheres to the following guidelines and codes:

- OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas(CAHRA)
- Responsible Jewellery Council (RJC) Code of Practice (CoP)
- London Bullion Market Association (LBMA) Responsible Gold Guidance
- DMCC Rules for Risk-Based Due Diligence in the Gold and Precious Metals Supply Chain
- Due Diligence Guidelines on Responsible Sourcing of Gold by the Ministry of Economy

4. SCOPE OF APPLICATION

4.1. The provisions, procedures, and controls detailed below shall apply to:

- All employees, if any, regardless of their function or location of work.
- All clients, including Buyers, Sellers, Refiners, Suppliers, Gold & Precious Metals Companies.

4.2. Employees of SR BULLION are responsible for ensuring that they comply with the standards established by local and international regulatory agencies. They are further expected to protect preventing SR BULLION and its reputation from being exploited for any illegal activity.

4.3. If any of SR BULLION'S employees or affiliates violate the provisions contained within this Policy, such violations will be treated as a disciplinary offence, and SR BULLION reserves the right to take any additional action that it, in its sole discretion, deems necessary to ensure the diligent and proper implementation and enforcement of this Policy.

4.4. If SR BULLION, its personnel, and/or premises are inadvertently used for money laundering or other illegal activities, SR BULLION can be subject to potentially serious civil and/or criminal penalties. Therefore, it is imperative that every member, officer, director, and employee is familiar with and complies with the processes and procedures set forth in this Policy.

4.5. If any client of SR BULLION is found to have breached any provisions of this Policy, then SR BULLION may take any of the following measures, in accordance with the severity of the violation:

- Warning.
- Temporary suspension of the operations of the Client's account.
- Termination of the Client's account.
- Reporting to the relevant Authorities.

5. POLICY CUSTODIAN

5.1. The Compliance Officer has been designated as the custodian of this Policy Manual for Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation Financing.

5.2. Although, the Compliance Officer is the custodian of the Policy, management at SR BULLION shall have responsibility for enforcement of this Policy within the organisation and with its clients.

6. PERIODICAL REVIEW

6.1. This AML/CFT/CPF Policy shall be reviewed on at least an Annual basis. Any review shall take into consideration legislative changes regarding AML/CFT/CPF and shall also examine the previous twelve months' implementation of the Policy, how the implementation may be improved, and any subsequent comments made during periodical checks by relevant authorities. Any amendments made to the Policy must have received prior written sign-off from the SR BULLION Senior Management, and or Team, whereupon they shall take effect immediately.

7. SR BULLION SERVICES

7.1. SR BULLION is a Free Zone Company registered with the Dubai Multi Commodities Centre, Dubai, UAE, since 24th of January 2023, holding Trade License No. DMCC-874338. The Company is exclusively engaged in jewellery trading, non-manufactured precious metal, pearls and precious stones trading, watches trading, import, export, and trading of raw gold and other precious metals. SR BULLION is a customer-centric organisation, committed to delivering high-quality, end-to-end services tailored to meet the diverse needs of its clients.

7.2. There are procedures in place to ensure that if a cash transaction exceeding UAE Dirhams 55,000 does occur, it will be reported promptly through the goAML Portal in accordance with the regulatory requirements.

7.3. SR BULLION's head office is located at Unit No: AG-PF-225, AG Tower, Plot No: JLT-PH1-I1A, Jumeirah Lakes Towers, Dubai, UAE. SR BULLION ensures a consistent and responsible supply of high-value precious metals for its clients' physical trading requirements. Moreover, SR BULLION has taken proactive steps to align with regulatory requirements.

7.4. The principal business activity of the company is import, export, and trading of raw gold and other precious metals.

7.5. The Company is registered on the Financial Intelligence Unit's goAML portal and is also registered with the website of the Executive Office for Control and Non-Proliferation (EOCN). This enables it to receive regular notifications pertaining to the inclusion or removal of entities/individuals from terrorist lists. This registration showcases SR BULLION' commitment to compliance with regulations aimed at controlling and prohibiting proliferation. SR BULLION ensures to take appropriate action whenever any such notification is received.

8. GOVERNANCE OF RISK: THREE LINES OF DEFENCE

8.1. To mitigate and control the risk involved, the AML programme at SR BULLION will create three lines of defence.

- **Operations**: This is the first line of defence. As the frontline for Know Your Customer (KYC) and Customer Due Diligence (CDD), the Company will handle customer onboarding, identification, and due diligence – all processes that require the collection and analysis of immense amounts of data, primarily acquired through lengthy customer questionnaires and investigations.
- **Compliance**: This is the second line of defence. It constitutes functions that oversee risks. The Compliance Department will develop policies and procedures, devise customer questionnaires

and requirements, and maintain the technologies necessary to streamline KYC and CDD processes. Where deemed necessary, the Company may hire the services of specialist consultants to design the AML/CFT/CPF Policies and Procedures and to attend training to understand the regulatory regime and the process to be followed. The Company will also design the criteria to divide the clients into risk categories and monitor ongoing Suspicious Transactions, if any.

- **Internal Audit**: This is the third line of defence. This function provides independent assurance to determine if proper controls are established. SR BULLION may appoint an independent compliance internal audit reviewer to conduct a periodic review to ensure that KYC and CDD programmes are based on complete, correct information, and approved protocols have been followed at the time of customer onboarding and during the execution of transactions. In the event of any perceived gaps, the shortfall will be presented to the management, and a remediation action plan will be developed.

8.2. **AML/CFT/CPF Governance Elements**

The Company has a Policy to follow the below-mentioned approach to ensure a strong and effective AML/CFT/CPF compliance culture in the Company.

8.3. **Responsibilities of Senior Management**

Senior Management of the Company is committed to ensuring that an effective AML/CFT/CPF compliance programme is in place. Further, the senior management has clearly articulated their expectations with regard to the responsibilities and accountability of all staff members in relation to the AML/CFT/CPF compliance programme.

As part of this Policy, the Company has defined the responsibilities of the senior management as under:

- Appointing a qualified management level AML/CFT/CPF Compliance Officer, possessing appropriate competence and independence duly approved by the Supervisory Authority,
- Ensuring a robust and effective independent audit function is in place,
- Putting in place and monitoring the implementation of adequate management and information systems, internal controls, and policies, procedures to mitigate risks,
- Approval of internal policies, procedures, and controls, including customer acceptance,
- Reviewing and providing comments in relation to the CO's periodic reports to the relevant Supervisory Authority,
- Approving the establishment and continuance of High-Risk Customer Business Relationships and their associated transactions, including those with PEPs,
- Application of the directives of Competent Authorities regarding combating Money Laundering and Terrorism Financing.

9. POLICY GOVERNANCE

9.1. SR BULLION has established an AML/CFT/CPF Compliance Officer, who is responsible for the coordination and implementation of AML/CFT/CPF procedures within the company. The AML/CFT/CPF Compliance Officer has a wide-ranging mandate assigned, including the task of ongoing monitoring and coordinating the identification, assessment, and mitigation of the risks that SR BULLION is or might be exposed to pertaining to money laundering and terrorism financing. Hence, SR BULLION ensures that a strong and suitable AML/CFT/CPF structure is in place.

9.2. SR BULLION's AML/CFT/CPF Compliance Officer plans to hold at least four (4) regularly scheduled meetings each year to discuss AML/CFT/CPF matters, review action plans, and recommend follow-up actions based on outcomes of the reviews. The Compliance Officer shall try to conduct at least one (01) meeting each Quarter, but under no circumstances shall the gap between two (2) AML/CFT/CPF Compliance Officer meetings be more than six (6) months. The Compliance Officer shall discuss initiatives required to be undertaken to continually improve SR BULLION's accomplishments within the AML/CFT/CPF area.

9.3. The AML/CFT/CPF Compliance Officer shall maintain written minutes or other records of its meetings and activities. Minutes of each meeting of the Compliance Officer shall be distributed to every member of the Compliance Team.

9.4. The Compliance Officer's key responsibilities will be as follows:

- To prepare a Policy and process Manual for implementing the provisions of the UAE's Federal (10) of 2025 on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation Financing, and Cabinet Resolution No. (134) Of 2025.
- To ascertain the proper implementation and effectiveness of the procedures and processes for fighting money laundering and terrorism financing operations within SR BULLION's.
- To prepare the staff training programme on the methods of controlling financial and banking operations, in accordance with the control procedure guide, and with other legal and regulatory texts in force.
- To review the above-mentioned procedures and processes periodically and develop them in line with up-to-date methods and guidance established on combatting money laundering and financing of terrorism.
- To periodically assess the Company's approach to risk identification, assessment, and mitigation plans for the principal legal and regulatory compliance risks facing the company and review the results of it.
- To prepare an effective customer identification and due diligence programme for onboarding a new customer, as well as updating CDD throughout the entire relationship with the customer.
- To periodically review resources, systems, and tools that are available to the Compliance Officer and ensure that up-to-date with the current international and national standards and are appropriate to the nature, size, and complexity of the business.
- To review findings of the internal audit and suggest necessary modifications to the Compliance Programme.
- To review ongoing challenges/issues in the implementation of the AML/CFT/CPF procedures and processes and ensure that proper controls are in place to mitigate/solve them.
- To take corrective/preventive actions if any gaps are identified.
- To discuss information about current and emerging legal and regulatory compliance risks and enforcement trends that may affect the Company's business operations, performance, or strategy.
- To review the reports submitted by the Compliance Unit on adopted procedures, unusual operations, and high-risk customers.
- To define the procedures and processes to be followed by the senior management team for approving business relationships with high-risk customers or when executing high-risk transactions.
- To discuss developing internal programmes focussed on promoting an ethical culture within the organisation.

- To review any data suggesting significant non-compliance involving any of the Company's officers or staff. The Compliance Officer will report to the Money Laundering Reporting Officer any data suggesting significant non-compliance that could affect the Compliance Programme or the Company.
- To review on a regular basis the company's significant risk exposures or compliance violations and the steps that have been taken to monitor, correct, and/or mitigate such violations or risks.
- To discuss the following areas and decide whether any actions need to be taken:
  - Updates on Sanctions
  - Notices / Circulars received from the Regulatory Authority
  - Suspicious Activity Reports (SARs) raised during the Quarter
  - Enhanced CDD conducted during the Quarter
  - Training conducted and attendance records of the staff
  - Feedback / Queries received from the Regulatory Authority
  - Pattern Analysis conducted during the Quarter
  - Any new risks associated with AML/CFT/CPF that are identified.

10. ROLE OF THE COMPLIANCE OFFICER/MONEY LAUNDERING REPORTING OFFICER

10.1. The ultimate responsibility for proper supervision, reporting, and compliance pursuant to AML/CFT/CPF shall rest with SR BULLION and its senior management.

10.2. The Head of the AML/CFT/CPF - Compliance Officer will be responsible for the following:

- Oversight of all compliance related activities at SR BULLION.
- Establishing transparency, honesty, and integrity throughout the business activities.
- Implement a robust compliance program across all its products, services, suppliers, customers, jurisdictions of operation, and delivery channels, including digital and physical transaction platforms.
- Ensuring that SR BULLION has in place adequate screening procedures to ensure high standards when appointing or employing officers or employees.
- Approving the overall business risk assessment for SR BULLION.
- Reviewing the quarterly compliance report along with high-risk areas in case an internal audit review is conducted.
- Ensuring that all employees of the organisation are being trained on the AML/CFT/CPF.
- Preparing, Approving, and Implementation of the Compliance Policy of the Organisation.
- Reviewing any issues identified during the CDD process and resolving them in a timely manner.
- Developing a good knowledge of all applicable Laws, Rules, Regulations, Notices, and the Standards related to the Precious Metals and Stones industry in the UAE.
- Setting the tone of zero tolerance against fraud.

10.3. SR BULLION has appointed Ms. Anam Tayyaba to act as authorised Money Laundering Reporting Officer (MLRO) of the Company. The MLRO will also be responsible for:

- Creating and implementing the AML/CFT/CPF compliance programme for SR BULLION and ensuring compliance with AML/CFT/CPF Laws, Regulations, Notices, the Standards, and international laws.
- Establishing and maintaining AML/CFT/CPF policies, procedures, processes, and controls in relation to the business of SR BULLION.
- Ensuring compliance by SR BULLION with the provisions of AML/CFT/CPF Guidelines, its

implementing rules and regulations, and SR BULLION's AML/CFT/CPF and KYC Policy.

- Reading any circulars, resolutions, instructions, and policies issued by the UAE Regulatory Agencies in all matters relating to the prevention of ML/CFT and Financing the proliferation of weapons and Illegal Organisations.
- Liaising between SR BULLION and UAE Regulatory Agencies in matters relating to compliance with the provisions of the AML/CFT/CPF Compliance Guidelines and its rules and regulations.
- Preparing and submitting to the UAE Regulatory Authorities written reports on SR BULLION's compliance with the provisions of the AML/CFT/CPF Compliance Guidelines and its implementing rules and regulations, in such form as the UAE Regulatory Agencies may determine, and within such period as the UAE Regulatory Agencies may allow in accordance with the AML/CFT/CPF Guidelines.
- Create a gap analysis document on existing AML/CFT/CPF Procedures and current Laws, Regulations, Notices, and the Standards of the UAE to determine the extent of the level of compliance and recommend actions if required.
- Attending the compliance training programme, particularly when any laws change.
- Raising Internal Suspicious Transaction alerts, if any, and investigating the matter along with presenting the findings to report all suspicious cases to the FIU.
- Reporting and filing Suspicious Transaction Report (STR) to FIU, if required
- Providing support and assistance to FIU with all the information it requires for fulfilling its obligations.
- Performing more extensive due diligence for high-risk customers and including proactive monitoring for suspicious types of activities.

10.4. The Compliance Function will be responsible for the following:

- Implementing SR BULLION's AML/CFT/CPF Policy and Procedures.
- Carrying out the compliance officer role to ensure that the functions are adhering to the regulations.
- Customer onboarding and KYC documentation.
- Conducting Customer Due Diligence and Enhanced Due Diligence.
- Liaising with other companies to obtain documents and information as required.
- Monitoring day-to-day transactions of SR BULLION for any unusual, structured, suspicious, and blacklisted ones.
- Monitoring trade-based money laundering and tracing structured transactions.
- Monitoring of suspicious accounts periodically.
- Reviewing and addressing the watch list and alerts. Update the blacklists on a regular basis.
- Liaising with the compliance department of other companies.
- Creating sound internal controls and monitoring adherence to them.
- Maintaining records as required by SR BULLION' AML/CFT/CPF Policy & Procedures.
- Taking proper remedial actions and informing the Senior Management if violations are identified.
- Reporting of unusual or suspicious transactions to the Senior Management.
- Educating the staff at SR BULLION regarding AML/CFT/CPF and 'Know Your Customer' procedures.

11. COMPLIANCE INTERNAL AUDIT

11.1. The Compliance Officer will conduct an internal audit to assess the effectiveness of the

AML/CFT/CPF Compliance and ensure its processes comply with regulatory requirements. The internal auditor will also play an important role in improving the controls by regularly tracking potentially identified weaknesses. Internal audit employees should have sufficient AML/CFT/CPF expertise and auditing experience. However, given the limited business transactions and small clientele/customers for the Company, an internal auditor may not be required immediately.

11.2. While conducting the Internal Audit, the Compliance Officer will have the following responsibilities:

- Conducting periodic assessment of relevant AML/CFT/CPF programme documentation (for example, KYC/CDD/Enhanced Due Diligence (EDD) policies and procedures and procedures related to identifying, investigating, and reporting suspicious transactions);
- Conducting testing of AML/CFT/CPF controls and processes carried out by the Company, such as KYC/CDD/EDD, training, suspicious-activity reporting, record keeping, and retention, among others.
- Conducting periodic evaluation of SR BULLION's AML/CFT/CPF Risk Assessment; and
- Following up on any remedial actions arising from independent audit or regulatory findings.

12. PURPOSE & RATIONALE

12.1. The purpose of this Policy is to set out provisions, procedures, and controls as enacted by SR BULLION concerning Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism and Proliferation Financing ("CFT/CPF"). All relevant personnel at SR BULLION must be aware of its existence and the contents within the Policy and hold the personal and corporate responsibility to bring any AML/CFT/CPF concerns to the attention of the AML/CFT/CPF Compliance Officer and/or any of its members.

12.2. The rationale behind the Policy is unequivocally clear. SR BULLION will only accept those Business Relationships:

- Whose sources of funds can be reasonably established as legitimate; and
- Who do not pose any risk (actual or potential) to SR BULLION's reputation and commitment towards AML/CFT/CPF.

12.3. SR BULLION will also ensure that all its staff is aware of the Policy and its contents, including the penalty for any non-compliance, and will not tolerate any involvement in illegal activities.

13. RISK FACTORS OF SPECIFIC CONCERN TO SR BULLION

13.1. The precious metals and stones sector offers opportunities for criminals seeking to conceal, transfer, and/ or invest their illicit proceeds. Like cash, precious metals and stones offer high value by weight, are difficult to trace and identify, and retain their value over time. Dealers in Precious Metals and Stones (DPMS), if they do not apply effective preventive measures, could be vulnerable to abuse by illicit actors engaged in laundering the proceeds of crime, financing of terrorism, arms trafficking, and sanctions evasion.

13.2. **Risks Associated with Precious Metals and Stones**

- Precious metals and stones are generally compact, durable, odourless, and of high value.
- Certain metals/stones (e.g., gold/diamond) are widely accepted as a method of exchange or

currency.

- Precious metals/stones retain their value over time and have roughly similar value all over the world.

In addition to these properties, precious metals and stones have characteristics that make them particularly attractive to criminals seeking to launder funds and others engaged in illicit behaviour:

- Differentiating precious metals and stones often requires laboratory techniques, so it can be difficult or impossible to track their movement.
- Precious metals and stones can be transformed (through re-cutting or recycling) into different objects while retaining their value, interrupting known custody and transfer chains.
- Purchase, sale, and exchange of precious metals often take place outside the formal financial system.

For these reasons, DPMS may be targeted by illicit actors seeking to abuse their services and exploit the advantages of precious metals and stones. Although most transactions involving DPMS are legal, these businesses may trade in items that could be the proceeds of crime, purchased with the proceeds of crime, and/or used to launder the proceeds of crime, unknowingly or complicitly.

DPMS poses a risk to SR BULLION. Complicit DPMS may knowingly partake in illicit activities and may, in turn, use their business relationships with SR BULLION to launder the proceeds of crime or carry out other illicit activity. Even DPMS that are not knowingly involved in illicit activities may use their accounts with SR BULLION to deal in the proceeds of crime.

13.3. Features of DPMS that Increase Risk

Not all DPMS pose equal risk. A DPMS is likely to be considered higher risk when it provides products or services that are attractive to illicit actors, has operations in high-risk jurisdictions, or does not apply appropriate anti-money laundering/combatting the financing of terrorism and proliferation financing (AML/CFT/CPF) controls.

13.3.1. Regulatory Environment

In many jurisdictions, DPMS are not required to comply with requirements related to the identification of customers and reporting suspicious activities. In other jurisdictions, these requirements are nominal. In jurisdictions where DPMS are not subject to effective supervision and enforcement, or where such oversight is weak, compliance measures are often inadequate. Even in jurisdictions with robust regulations, these requirements typically apply only to DPMS engaging in cash transactions above a certain value threshold. Where DPMS are unregulated or under-regulated, they are unlikely to implement effective measures to protect themselves from abuse.

In contrast, an effective AML/CFT/CPF framework and supervisory regime for DPMS can protect DPMS by effectively imposing AML/CFT/CPF requirements and by detecting, deterring, and prosecuting ML/TF crimes. It is important to note that certain DPMS in the UAE are required to comply with all requirements of the AML-CFT Decision, including the requirement to perform Customer Due Diligence (CDD) and report suspicious transactions.

13.3.2. Products, Services, and Delivery Channels

Products, services, and delivery channels that facilitate the rapid, efficient, anonymous movement of value on a large scale will be more attractive to illicit actors and may put a DPMS at a higher risk of abuse. Such products, services, and delivery channels may include:

- Products (such as bullion and uncut stones) that are particularly hard to trace, retain, or even increase in value despite being transformed into new forms (melted down, re-cut, etc.), and offer high value by weight.
- Services, such as metal accounts, that allow customers to rapidly purchase and sell precious metals.
- Delivery channels that allow transactions to be carried out quickly and anonymously, such as accepting cash or virtual assets and conducting transactions online or through intermediaries.

13.3.3. **Customer Base**

The types of customers that a DPMS serves can also impact risk. For example, a DPMS that primarily deals with PEPs may be higher risk than one that serves a lower-profile clientele.

13.3.4. **Geography**

DPMS may be based, or may trade internationally, in jurisdictions that are higher risk for money laundering, the financing of terrorism, and the financing of proliferation. Such DPMS may pose a heightened risk to LFIs. Higher-risk jurisdictions may be characterised by:

- A low level of government oversight and regulation of the precious metal and stone value chain;
- Low economic and political stability;
- High use of the informal banking system;
- High levels of corruption;
- The presence of terrorists and other non-state armed groups;
- Weak border control measures; and/or
- Sanctions and embargoes

13.4. **ML/TF/PF Risks to be considered by SR BULLION:**

When required to apply AML/CFT/CPF measures, SR BULLION should carefully consider factors such as customer risk, geographic risk, channel risk, and product, service, and transaction risk. Consideration should be given to such factors as:

- Country of origin of the Precious Metals and Stones (PMS) — Particularly in relation to whether the country is a known production or trading hub for the type of PMS; has adequate regulations and controls; is 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 organisations).
- Country of origin or residence status of the counterparty or customer (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country), particularly in relation to locations where the transaction is conducted, and the goods are delivered.
- Channel by which the counterparty/customer 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).

- Type, nature, and characteristics of the products and/or services, including but not limited to quantity, quality/level of purity, price/value, form (whether physical or virtual, raw/rough or processed/finished, etc.), rarity, portability, potential for anonymity.
- Type, size, complexity, cost, and transparency of both the transaction (including whether the physical or virtual exchange of merchandise is involved) and the means of payment or financing—particularly in relation to whether they appear to be consistent with the counterparty or customer's socio-economic profile, local market practices, and the degree of expertise required.
- Use of complex trade structures, unnecessary intermediaries, front companies, or opaque ownership arrangements without clear commercial justification.
- Inconsistencies or anomalies in trade documentation, including discrepancies between invoices, contracts, shipping documents, quantities, values, or descriptions of goods.

14. PROCEDURES AND CONTROLS (GENERAL)

14.1. SR BULLION is required to establish and implement internal control procedures aimed at preventing and impeding money laundering, financing of terrorism, and Proliferation Financing. This Policy contains, as an integral part of it, certain procedural checks and balances (collectively "Procedures and Controls") to ensure the vigilant and effective operation of the Policy.

14.2. Such procedures shall, among other things, ensure that all stakeholders are aware of the provisions of the law, its implementing rules, and regulations, as well as all reporting and control procedures established by SR BULLION and the supervising authority.

14.3. SR BULLION shall see to it that their respective policies and procedures for dealing with AML/CFT/CPF are clearly set out and reflected in their operating manual.

14.4. The Procedures & Controls are as follows:

- Identification, Verification, and Know-Your-Customer ("KYC") and updating of KYC information
- Activity Monitoring
- Reporting of Suspicious Activities
- Training and Awareness
- Record Keeping

15. IDENTIFICATION, VERIFICATION AND KNOW YOUR CUSTOMER

15.1. Identification (ID), Verification (VR), and Know-Your-Customer (KYC) are effective defences against money laundering and/or financing of terrorism, and all together, form the first key step in the Procedures and Controls. Carrying out ID, VR, and KYC procedures is mandatory.

15.2. SR BULLION shall establish, document, and maintain a written identification, verification, and KYC programme (hereinafter referred to as "Customer Identification Programme") appropriate for its size and business that, at a minimum, includes each of the requirements under the KYC Checklist. The Customer Identification Programme shall be part of SR BULLION's AML/CFT/CPF compliance programme.

15.3. SR BULLION shall obtain and record competent evidence of the true and full identity of the client, Ultimate Beneficiary Owner, representative capacity, domicile, legal capacity, occupation, or business purposes of clients, as well as other identifying information on those clients, whether they be occasional or usual, using documents detailed in the KYC Checklist. Following applicant screening and background information check, along with review of business plan, source of funds, and expected levels of activity, an initial decision will be made with respect to the application status. This includes whether the client may be accepted, rejected, or whether more information may be required.

15.4. Clients should be made aware of the SR BULLION's explicit policy that business transactions will not be conducted with applicants who fail to provide competent evidence of their activities and identity, but without derogating from SR BULLION's legal and ethical obligations to report suspicious transactions. Where initial verification fails to identify the applicant or give rise to suspicion that the information provided is false, additional verification measures should be undertaken to determine whether to proceed with the business transaction. Details of the additional verifications are to be recorded.

15.5. If during the business relationship, SR BULLION has reason to doubt

- the accuracy of the information relating to the customer's identity; or
- that the customer is the beneficial owner; or
- the intermediary's declaration of beneficial ownership; or
- If there are any signs of unreported changes,

SR BULLION shall take further measures to verify the identity of the customer or the beneficial owner, as applicable. Such measures may include the following:

- Referral of names and other identifying information to criminal investigating authorities; and
- Review of disciplinary history and disclosure of past relevant sanctions.

15.6. The Customer Identification Programme must include procedures for responding to circumstances in which the Compliance Monitoring Team cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe, among others, the following:

- When SR BULLION should not do business with a client
- The terms under which a customer may conduct business transactions while SR BULLION attempts to verify the customer's identity.
- When SR BULLION should file a Suspicious Activities / Transaction Report

15.7. The Customer Identification Programme must include procedures for providing customers adequate notice that SR BULLION is requesting information to verify their identities.

15.8. In rare events or incidences where a Customer fails to provide adequate KYC information or appears hesitant/unwilling to provide information as required to establish adherence to KYC norms, SR BULLION shall not proceed with a transaction for such a Customer and flag the case as a High-Risk customer. Such cases are marked for reporting to the Regulator through Suspicious Transaction Report (STR), and for increased monitoring.

16. CUSTOMER ONBOARDING

16.1. In general, SR BULLION will have the following as its customers:

- Natural persons
- Legal persons, including individual members of corporations.

16.2. Natural persons and individual members of the corporate customers:

16.2.1. SR BULLION shall obtain from all individual members of corporate customers, including shareholders, beneficial owners, directors, managers, authorised signatories, power of attorney holders, and other key managerial people, the following information:

- Individual's full name (as per passport)
- Date and place of birth
- Nationality
- Passport Number
- National Identity Document (Emirates ID, for the UAE nationals/residents)
- Physical Address (residential and business/home country and the UAE)
- Contact details.
- Source of funds and wealth
- Declaration regarding Beneficial Ownership, that is, the person who has ultimate ownership.
- Whether the customer is a Politically Exposed Person (PEP) or a Close Associate of a PEP

The above list is a summary of the information required. A detailed checklist is attached in Appendix A.

16.2.2. As part of the process for identifying and verifying customers, and for authenticating the original documents upon which the verification is based, SR BULLION will include procedures for the certification of the customer identification and address documentation it obtains. SR BULLION shall request members of corporate clients to produce or show the original documents for verification purposes. Such procedures will encompass:

- Certification by employees (for example, by including the name, title of position, date, and signature of the verifying employee(s) on the copies of documents maintained on file, along with a statement representing that the copy of the document is a "true copy of the original") and/or,
- Third parties (for example, by including the name, organisation, title of position, date, and signature of the verifying person, along with a statement representing that the copy of the document is a "true copy of the original").

If physical verification is not possible, or the customer is not in the UAE, SR BULLION staff may do the verification of original ID on a secured video platform such as Zoom or Google Meet and store a screenshot of evidence of verification.

16.2.3. For individual, in case the original ID documents cannot be presented for verification, a duly authenticated document by the UAE Embassy in the home country of the individual or duly attested documents by a UAE Notary Public in case the individual is in the UAE can be acceptable in place of the original documents. In cases where documents are obtained from foreign sources in countries that are members of the Hague Apostille Convention, SR BULLION may request documents certified by an Apostille seal.

16.3. **LEGAL PERSONS**

16.3.1. Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound up, or terminated. In case of doubt as to the veracity of the corporation or identity of its directors and/or officers, or the business or its partners, a search or inquiry with the relevant Supervising Authority/Regulatory Agency shall be made.

16.3.2. SR BULLION shall obtain from all corporate customers the following information:

- Incorporated name
- Shareholders (To include 'active' and 'silent' or 'sleeping' partners)
- Ultimate Beneficial Owners (UBO) (the Beneficial Owner shall be whoever person that ultimately owns or controls, whether directly through a chain of ownership or control or by other means of control such as the right to appoint or dismiss most of its Directors, 25% or more of the shares or 25% or more of the voting rights in the Legal Person)
- Managers (That person having day-to-day control of the company, if not a shareholder/partner)
- Authorised Signatories
- Passport of all shareholders, Ultimate beneficial owners, Managers, and Signatories
- National Identity Document of shareholders, UBOs, Managers, Signatories (Emirates ID, if a customer is a resident/citizen of the UAE).
- Memorandum and Articles of Association.
- Power of Attorney (if applicable).
- Proof of physical address of the company
- Contact details
- Business activities (type and volume)
- Source of funds and wealth
- Tax registration number of the corporate entity

The above list is a summary of the information required. A detailed checklist is attached in Appendix B.

16.3.3. As part of the process for identifying and verifying customers, and for authenticating the original documents upon which the verification is based, SR BULLION will include procedures for the certification of the customer identification and address documentation it obtains. SR BULLION shall request corporate clients to produce or show the original documents for verification purposes. Such procedures will encompass:

- Certification by employees (for example, by including the name, title of position, date, and signature of the verifying employee(s) on the copies of documents maintained on file, along with a statement representing that the copy of the document is a "true copy of the original") and/or,
- Third parties (for example, by including the name, organisation, title of position, date, and signature of the verifying person, along with a statement representing that the copy of the document is a "true copy of the original").
- In addition, where a customer has a nominal manager, nominee shareholder, or bearer shareholder, SR BULLION shall require disclosure of such status and obtain relevant information identifying the nominee, representative, or person acting on behalf of another. Customers shall be required to notify SR BULLION of any changes to such information within fifteen (15) working days of the change, in line with applicable legal

requirements, as a measure to prevent and mitigate the risk of financial crime.

If physical verification is not possible, or the customer is not in the UAE, SR BULLION staff may do the verification of original ID on a secured video platform such as Zoom or Google Meet and store screenshot of evidence of verification.

16.3.4. For companies or businesses, in case the original ID documents are not available, a duly authenticated document by the UAE Embassy in the home country of the Company or duly attested documents by a UAE Notary Public in case the Company is in the UAE can be acceptable in place of the original documents. In cases where documents are obtained from foreign sources in countries that are members of the Hague Apostille Convention, SR BULLION may request documents certified by an Apostille seal.

16.3.5. SR BULLION shall take additional care in dealing with cases where customer verification is done without face-to-face contact with the ultimate client for corporate customers.

17. KYC PROCESS

17.1. SR BULLION maintains clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher risk than average risk. Before accepting a client, KYC and due diligence procedures are followed by examining factors such as the customer's background, country of origin, public or high-profile position, business activities, or other risk indicators.

17.2. In case of retail Business SR BULLION will carry on Simplified Due Diligence on all Low-risk clients and if in case any retail Business transaction exceeds AED 55,000 (whether as a single transaction or Multiple Transactions) in that case Complete Customer Due Diligence process shall be followed.

17.3. KYC is to be carried out according to the mandatory Customer KYC checklist:

- Natural Person and Individual Members of Corporate Client KYC Checklist (Refer to Appendix A)
- Legal Person (Corporate) KYC Checklist (Refer to Appendix B)

17.4. SR BULLION should be required to conduct the KYC and CDD procedure when:

- Establishing a new business relationship.
- Carrying out occasional transactions above the applicable designated threshold.
- There is suspicion of money laundering or terrorist financing.
- If SR BULLION has doubts about the veracity or adequacy of the previously obtained customer identification data.
- It is necessary to obtain additional information from existing customers based on the conduct of the account.
- When there are changes to signatories, mandate holders, beneficial owners, and other relevant key personnel.

If the customer is unable to comply with these requirements, SR BULLION should:

- Not open the account, commence business relations, or perform the transaction.
- Terminate the business relationship.
- Consider filing a suspicious-transaction report in relation to the customer.

17.5. SR BULLION is strictly forbidden to do business with shell companies. Shell companies shall mean an institution that has no physical presence in any country, no active business and which merely exists on paper.

17.6. An integral part of the KYC process is the carrying out of customer screening and relative risk assessment. Screening ensures that a customer is not listed on the official sanction's lists issued by the Government and law enforcement agencies. Background checking is designed to identify any adverse information about the past conduct of an individual that may influence their suitability as a customer.

17.7. When conducting the KYC process, there shall be no reliance on third-party information or "hearsay". For applicants introduced to SR BULLION by a third party, SR BULLION must carry out and perform all identification, verification, and KYC procedures.

17.8. It should be borne in mind that KYC is more than a procedure and is a discipline that is to be developed. For example, KYC should become second nature so that any significant information related to the customer obtained during meetings, telephone discussions, visits, online search, etc., and which is deemed to be relevant for the Policy, should be recorded. Fresh due diligence should be undertaken, especially if it appears that the veracity or accuracy of previous information is doubted.

18. RISK-BASED APPROACH

18.1. A risk-based approach is one of the most effective ways to protect against money laundering and terrorist financing. It is imperative to understand that certain risks associated with various elements of a customer's profile may be indicative of potential criminal activity. This may include geographical and jurisdictional issues, business and product types, distribution channels, and prevailing transaction types and amounts.

18.2. Customers will be reviewed, assessed, and allocated an appropriate level of risk of money laundering, divided into High, Medium, or Low Risk.

- High-risk customers will be subject to enhanced levels of due diligence that go beyond the core policies and principles contained in this Policy.
- Medium-risk customers will be subject to the core Policies and Procedures contained within this Policy.
- Low-risk customers may be subject to certain flexibility within the procedures contained in this policy. However, care should be exercised to ensure that the Company continues to meet its legal obligations.

18.3. Although it is generally accepted that failure to provide satisfactory due diligence documentation might be indicative of a money laundering concern, it is also recognised that, due to the geographic diversity of businesses, on occasion, it might prove difficult or impossible to obtain documentation that exactly meets the criteria set out within this Policy.

18.4. If the situation mentioned in the Clause above occurs, and there are no reasons to suspect money laundering, the customer documentation should be communicated to senior management together with an explanation detailing the types of issues that arose. Senior management, in

consultation with the Compliance Officer, will then review the documentation and consider the risks associated with acceptance of identification evidence that falls outside these procedures, thereafter, providing the personnel with advice and guidance, as appropriate.

18.5. The risks considered in the assessment and decision process, and the conclusions reached should be properly documented within the customer KYC file, with appropriate sign-off by the individuals involved. Only Senior Management, in consultation with the Compliance Officer, may determine the High-risk level to be attributed to any customer or/ and approve documentation that does not meet the exact requirements of the Company's anti-money laundering Policy.

18.6. All customers are subject to a risk assessment and risk ratings will be recorded in the file. Due diligence requirements must be commensurate with the risk level associated with the customer and enhanced due diligence will be necessary for all higher risk customers.

18.7. In addition to trigger-based reviews, SR BULLION shall conduct periodic reviews of the Customer's KYC and conduct CDD based on the risk profile of the customer:

- High Risk Customers: Every 12 months
- Medium Risk Customers: Every 18 months
- Low Risk Customers: Every 24 months

If there is no transaction with a particular account for 6 months, then the account is marked as Dormant and Re-KYC is performed once the client wants to reinitiate the transaction after 6 months.

In relation to customers who did not trigger an alert, SR BULLION may consider refreshing required information and conducting a simplified due diligence by asking the customer to confirm baseline information on file along with documentary proofs.
For customers who triggered an alert, an in-depth assessment of the customer activity may be required.

19. ENHANCED DUE DILIGENCE

19.1. A High-Risk Customer presents a higher-than-normal adverse risk of involvement in money laundering, financing of terrorism, Proliferation Financing or any other matter that the Senior Management or the Compliance Officer considers to be significant.

19.2. To mitigate the risks associated with High-Risk Customers, it will be necessary to consider the application of a level of enhanced due diligence for those customers. SR BULLION' Senior Management, in consultation with the MLRO, will determine whether the level of risk is acceptable.

19.3. Enhanced Due Diligence ("EDD") will need to go beyond the normal requirements applied to the approval and monitoring of customers, as contained within this Policy. As the reasons for designation as high risk will vary from customer to customer, the nature and level of enhancement will need to be determined separately as and when high-risk customers are identified, and procedures will need to explain how the increased risks will be minimised.

19.4. Should it be determined that a customer who fulfils the criteria for designation as high risk does not warrant enhanced due diligence, the reasons for the decision and the way the risks are

mitigated should still be fully documented and placed in the customer's file.

19.5. In addition, any EDD procedures carried out during the approval process, together with proposed procedures for future monitoring, should be fully documented and placed in the customer file.

19.6. SR BULLION shall perform Enhanced Due Diligence in the following scenarios:

- Customers from High-risk countries.
- Politically Exposed Persons (PEPs) and Close Associates of PEPs.
- If the customer/transaction is found to be suspicious/unusual.
- Any other suspicious cases are alerted based on the rule violation(s).

The above scenarios are reviewed periodically and updated as required through the Quarterly Compliance Officer.

20. POLITICALLY EXPOSED PERSONS (PEPS)

20.1. A Politically Exposed Person or PEP is a term that is used to describe individuals who are, or have been, entrusted with prominent public positions, who can be susceptible to bribery and corruption. The following list contains examples of persons who may be considered PEPs, although this list should not be viewed as exhaustive:

- Current and Ex-Head & Deputy Head of state or National Government (President, Prime Minister, Government Ministers, Provincial Governors, Cabinet Members, their Deputies (assistants), Senior Ministerial staff, and Secretaries.
- Current and ex-Members of National and Provincial Assemblies and Senate.
- Senior Civil Servants, including Senior Government Officials, Heads of Government Departments, and the Police Service.
- Senior Judicial & Military officials
- Senior Executives of state-owned Corporations.
- High-ranking Officers in Diplomatic Service (Ambassadors, High Commissioners, Envoys, Attachés, Consul Generals, Consuls, Honorary Consuls, Counsellors, etc.)
- Senior Political Party Officials and functionaries such as Leader, Chairman, Deputy leader, Secretary General, and Compliance officer or any other Senior ranks in the party (does not include middle-ranking or more junior individuals).
- Close family members of PEPs, including spouses, children, parents, siblings, and may also include other blood relatives and relatives by marriage.
- Closely associated persons, including close business colleagues and personal Advisors / Consultants to the politically exposed person, as well as persons who are expected to benefit significantly by being close to such a person.

20.2. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused to commit money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as conducting activity relating to terrorist financing (TF) or find that their public position has been unknowingly used or is being unknowingly used, for their benefit or benefit of others who may be involved in illegal activities such as corruption, bribery, fraud etc.

20.3. Risk is increased considerably when a PEP is located in a high-risk country.

20.4. SR BULLION will ensure that each beneficial owner or controller is not a PEP by performing searches on official databases to screen names against its database or by referring to publicly available information. The results of such verification will be recorded within the customer KYC file.

20.5. If a PEP is identified, SR BULLION will:
- Assign a rating of high risk to the customer.
- Complete PEP Report, ensuring that the Senior Management approves establishing a business with the customer.
- Conduct enhanced due diligence and be vigilant in monitoring the business relationship.
- Ensure reasonable measures will be taken to establish the source of wealth/funds.
- Track PEP relationships for the purposes of reporting and monitoring.

21. TARGETED FINANCIAL SANCTIONS (TFS)

21.1. SR BULLION will take all the required steps to ensure that all customers with whom a business relationship is established are screened against relevant notices such as:
- United Nations sanctions (UN)
- UAE (Local Terrorist List)
- the Office of Foreign Assets Control (OFAC)
- Her Majesty's Treasury Department – UK (HMT)
- European Union sanctions (EU)

21.2. Screening shall also cover Proliferation Financing (PF) designations in accordance with Federal Decree-Law No. (10) of 2025. SR BULLION shall identify, assess, and mitigate PF risks arising from clients, suppliers, and transactions. Any suspicion or reasonable grounds to suspect PF activities shall be reported to the UAE Financial Intelligence Unit (FIU) via the goAML portal in the same manner as Money Laundering or Terrorism Financing suspicions.

21.3. Any confirmed matches to sanctions lists will result in the decline of a business relationship, and the necessary reports will be made to the Financial Intelligence Unit (FIU).

21.4. SR BULLION shall document and record all the actions that were taken to comply with the sanction's regime, including PF-related measures, and the rationale for such action. Compliance officer will consider if any further action is required such as freezing of funds.

21.5. Targeted Financial Sanctions (TFS) Obligations :
a. SR BULLION is registered on the goAML portal and with the Executive Office for Control and Non-Proliferation (EOCN) to receive official notifications relating to the inclusion or removal of persons and entities from the Targeted Financial Sanctions (TFS) Lists, in compliance with Cabinet Resolution No. (74) of 2020.
b. SR BULLION ensures ongoing compliance with TFS requirements by subscribing to sanctions updates issued by the EOCN through its official website. The Compliance Officer shall maintain the subscription using the Company's official email address.
c. Upon any update issued by the EOCN (including additions to or removals from the Local Terrorist List), notifications shall be received by the subscribed email address.
d. Upon receipt of an EOCN notification, the Compliance Officer shall, without delay:
- Screen all existing customers and beneficial owners against the updated sanctions list;
- Conduct screening using automated and/or manual screening methods, as appropriate; and

- Maintain a sanctions screening log recording the date of screening, results, and any action taken.

e. Reporting to EOCN :
If a positive or potential match is identified, the Compliance Officer shall:

- Report the match to the EOCN using the prescribed TFS Reporting Form available on the EOCN website;
- Submit the report within 24 hours of identification; and
- Comply with all instructions issued by the competent authority, including freezing of funds or other measures, where applicable.

f. Where no match or relationship is identified, a "No Match / No Relationship" response shall nevertheless be submitted via the prescribed EOCN reporting form.

g. Any confirmed match to a sanctions list shall result in the decline or termination of the business relationship, and the necessary reports shall be submitted to the Financial Intelligence Unit (FIU) in accordance with applicable laws and regulations.

h. SR BULLION shall document and retain records of all actions taken to comply with the sanctions regime, including TFS-related measures and the rationale for such actions. Senior Management shall consider whether any further action is required, including the freezing of funds or assets.

22. UPDATING KYC INFORMATION

22.1. KYC is an ongoing process. The foundation of any customer due diligence and monitoring procedures lies in the initial collection of KYC information and the ongoing updating of that information.

22.2. SR BULLION will take reasonable steps to ensure that KYC information and documents are updated as and when required.

22.3. As a minimum standard, KYC information must be updated ongoing for business relationships.

23. MONITORING OF CLIENT'S ACTIVITIES

23.1. With regard to established Business Relationships, SR BULLION is required to undertake ongoing supervision of customers' activity, including auditing transactions executed throughout the course of the relationship to ensure that they are consistent with the information, types of activity, and risk profiles of the customers.

23.2. In the case of customers or Business Relationships identified as high risk, SR BULLION will investigate and obtain more information regarding the purpose of transactions that are to be conducted; and enhance ongoing monitoring and review of transactions to identify potentially unusual or suspicious activities. Ongoing Monitoring is performed by using the software known as LSEG World Check Software.

23.3. In keeping with the level of risk involved, SR BULLION will evaluate the specifics of the transactions examined concerning to the customer's due diligence information or profile, and obtain sufficient information on the counterparties and/or other parties involved (including but not limited to information from public sources, such as internet searches), to determine whether the transactions appear to be:

- Normal (that is, the transactions are typical for the customer, for the other parties involved, and for similar types of customers).
- Reasonable (that is, whether the transactions have a clear rationale and are compatible with the types of activities that the customer and the counterparties are usually engaged in).
- Legitimate (that is, whether the customer and the counterparties are permitted to engage in such transactions, such as when specific licenses, permits, or official authorisations are required).

24. INDICATORS OF SUSPICIOUS ACTIVITIES – RED FLAGS

24.1. Methods which criminals utilise to conduct money laundering, financing of terrorism and financing of proliferation financing are constantly evolving, and as such, in many cases, there exist particularities within a given market or given type of trust and company service that may be beyond the scope of red flags identified within this Policy. Therefore, the following list of red-flag indicators of potentially suspicious transactions should by no means be treated as exhaustive.

It is noted that the presence of one or more of the indicators below does not necessarily mean that a transaction involves ML/FT. However, it is an indication that enhanced due diligence, or further investigation may be required, so that an appropriate determination can be made by SR BULLION' appointed Compliance Officer as to whether the transaction can be deemed suspicious or not.

24.2. A red flag should be raised with respect to trade practices in the following circumstances:

- Precious metals/stones originate from a country where there is limited production or no mines at all.
- Trade in large volumes conducted with countries that are not part of a specific precious metals and stones pipeline.
- An increase in the volume of the activity in a DPMS account despite a significant decrease in the industry-wide volume.
- Selling or buying precious metals and stones between two local companies through an intermediary located abroad (lack of business justification, uncertainty as to actual passage of goods between the companies).
- Volume of purchases and/or imports that grossly exceed the expected sales amount.
- A single bank account is used by multiple businesses.

24.3. A red flag should be raised with respect to the Business Relationship, or the Customer in the following circumstances if the customer:

- Suddenly cancels the transaction when asked for identification or information.
- Is reluctant or refuses to provide personal information, SR BULLION 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 are they conducting their activities in a certain manner
  - who they are 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).
- 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 SR BULLION.
- Is located a significant geographic distance away from SR BULLION, 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 SR BULLION or its employees.
- Is prepared to pay substantially higher fees than usual, without a 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 that 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 PMS 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 the 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 authorised 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 shortcuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Requests 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 that appear to be falsified or forged.
- Requires that transactions be processed 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, to preserve their anonymity, without adequate and reasonable explanation.

24.4. A red flag should be raised with respect to the transaction if it:

- 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 (especially gold) or jewellery for cash in small incremental amounts.
- Involves the barter or exchange of PMS (especially gold) or jewellery for other high-end jewellery.
- Appears structured 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.
- Involve 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 PMS 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 authorised 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).
- 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 that, 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;
- Insist on an unusually quick completion, without a reasonable explanation.
- Takes place through intermediaries who are foreign nationals or individuals who are tax non-residents.
- 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).

24.5. A red flag indicator for means of payment:

- 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 traveller's cheques,
- Cashier's cheques and money orders in round denominations (to keep below the reporting threshold limit) to pay for PMS. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information.
- Is divided into smaller parts or instalments 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.

25. REPORTING OF SUSPICIOUS ACTIVITIES

25.1. SR BULLION shall institute a system for mandatory reporting of suspicious transactions pursuant to the UAE AML/CFT/CPF legislative and regulatory framework. Any suspicious activities/transactions (SARs/STRs) or additional information required in relation to them shall be reported to the FIU

through the GOAML system. The same shall be filed within 5 working days after becoming aware of the suspicious transaction.

25.2. Where any employee or personnel, director, or officer of SR BULLION knows that the client has engaged in any of the predicate crimes, the matter must be promptly reported to the Head of Compliance.

25.3. The MLRO will review the matter and if sufficient evidence is available, then the matter will be escalated to the Senior Management to review and decide whether the matter needs to be reported to the FIU as Suspicious Activity.

25.4. If there are reasonable grounds to suspect that the customer has engaged in an unlawful activity, the Compliance Officer, on receiving such a report, must promptly evaluate whether there are reasonable grounds for such belief and then immediately report the case to the FIU, and records an opinion, that such reasonable grounds do not exist.

25.5. SR BULLION shall maintain a register of all suspicious transactions that have been brought to the attention of its Compliance Officer, including transactions that are not reported to the FIU. The register shall contain details of the date on which the report is made, the person who made the report to the Compliance Officer, and information sufficient to identify the relevant papers related to said reports.

25.6. SR BULLION acknowledges that failure to report a suspicious transaction, whether intentionally or by gross negligence, is a federal crime. Any person who fails to perform their statutory obligation to report a suspicion of money laundering, or the financing of terrorism or proliferation financing, is liable to a fine and/or imprisonment or both.

26. TYPES OF REPORTING ON GOAML PORTAL

26.1. **Funds Freeze Report (FFR)**

- Reporting entities are supposed to file the Funds Freeze Report to report any freezing measure, prohibition to provide funds or services, and any attempted transactions related to confirmed matches. This report is raised when the reporting entity finds a full match of the customer's name with a name listed in the UAE LOCAL LIST or UN CONSOLIDATED LIST.

26.2. **Partial Name Match Report (PNMR)**

- This report is raised when the reporting entity cannot verify if the name of the customer is a full match to the name of a sanctioned person listed in the UAE LOCAL LIST or UN CONSOLIDATED LIST.

26.3. **Suspicious Transaction/Activity Reporting (STR/SAR)**

- Transactions that do not match the customer profile, high volumes of transactions being made in a short period, payment of high amounts by cash, cannot provide identification documents and source of funds; these are some examples of suspicious activities/transactions.
- If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or a potential customer, a reporting entity suspects transactions or attempted transactions related to money laundering, fraud or terrorist financing, then the entity should submit an STR/SAR to the FIU at the earliest.

- File STR/SAR if a full/partial match of the customer's name is found on other international sanctions lists (e.g., OFAC, UKHMT, EU, etc.)
- If a reporting entity suspects or has reasonable grounds to suspect that funds/activity are the proceeds of a criminal activity, or are related to terrorist financing, it shall, as soon as possible but no later than 5 days, report promptly its suspicions to the Financial Intelligence Unit (FIU).

26.4. **High-Risk Countries Report / Activity (HRC/HRCA)**

- The obligation for reporting, as well as putting on hold, is for cross-border transactions through banking or remittance channels. These transactions may include transactions destined to, originated from, or being routed through jurisdictions that are classified as a 'High-Risk Jurisdiction subject to a Call for Action' by FATF. Currently, this includes the Democratic People's Republic of Korea, Iran, and Myanmar.
- Such reported transaction(s) may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the transaction within the set period.

26.5. **Dealers in Precious Metals & Stones Report (DPMSR)**

- Dealers in Precious Metals and Precious Stones (DPMS) are identified under UAE law as Designated Non-Financial Business and Professions (DNFBPs) when they carry out a single transaction or several transactions, interrelated in appearance, whose value is equal to or greater than AED 55,000.
- All cash transactions and international wire transfer Transactions with individuals/entities (B2C/B2B) equal or exceeding AED 55,000 need to be reported in DPMSR. Obtain and verify identification documents (ID or Passport) that need to be reported in DPMSR.

27. TIPPING OFF AND CONFIDENTIALITY

27.1. Tipping off a customer is an unauthorised act of disclosing information that:

- may result in the customer, or a third party (other than FIU) knowing or suspecting that the customer is or may be the subject of:
  - a suspicious transaction report; or
  - an investigation relating to money laundering or terrorist financing; and
- may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorist financing.

27.2. SR BULLION directors, officers, and employees shall not warn customers that information relating to them has been or is in the process of being reported to the FIU, or communicate, directly or indirectly, such information to any person other than the FIU. Any violation of this confidentiality provision shall render them liable for criminal, civil, and administrative sanctions under the UAE AML/CFT/CPF law.

28. TRAINING AND AWARENESS

28.1. SR BULLION shall provide education and training to all its staff and personnel, including directors and officers, to ensure that they are fully aware of their obligations and responsibilities in combatting money laundering and financing of terrorism and proliferation financing, and so that they are familiar the system in place for reporting and investigating suspicious matters.

28.2. SR BULLION may, due to the scale and nature of its operations, look to appoint an independent Internal Auditor or Trainer who has relevant experience and expertise in the field of AML/CFT/CPF.

28.3. SR BULLION shall, at least once a year, conduct refresher training to remind key staff and officers of their AML/CFT/CPF responsibilities and to make them aware of any changes in the laws, national and international, and rules relating to AML/CFT/CPF.

28.4. New employees will receive appropriate training within 30 days of their hire date. Training for all employees must include not only the legal elements of AML/CFT/CPF laws and regulations but should also cover job-specific applications of these laws. Ongoing training will be provided and updated regularly to reflect current developments and changes to laws and regulations.

28.5. To ensure the continued adherence to SR BULLION' AML/CFT/CPF and KYC policies and procedures, all employees are required to confirm their awareness of the contents of this Compliance Policy by signing the acknowledgment form annually, or more frequently.

28.6. Completion of AML/CFT/CPF training sessions by all employees, including details such as date of training, type of training (initial, refresher, job-specific), trainer's name, and mode of delivery (in-person, online, etc.).

28.7. Receipt of signed AML/CFT/CPF acknowledgment forms from employees confirming their understanding and adherence to the AML/CFT/CPF and KYC policies.

28.8. Training programs shall cover the new obligations introduced under Federal Decree-Law No. (10) of 2025, including Proliferation Financing (PF) risk awareness, governance responsibilities of senior management, and compliance requirements related to Virtual Assets and Virtual Asset Service Providers (VASPs). The Compliance Team shall review training content annually to ensure alignment with the latest Financial Intelligence Unit (FIU) and Ministry of Economy (MoE) guidance and circulars.

29. RECORD KEEPING

29.1. The following documents shall be considered as SR BULLION's AML/CFT/CPF Documents:

- All clients' documentation as provided in the KYC checklist and/or correspondences, including the documents obtained during CDD and/or EDD.
- All documentation concerning a suspicious activity report concerning a client or applicant, together with any response or follow-up.
- Records of AML/CFT/CPF training sessions attended by SR BULLION's staff, officers, and their affiliates, the dates, content, and attendees.
- Records of all AML/CFT/CPF decisions taken by the senior management.
- All records, documents, and data for all financial, cash, and local or international commercial transactions and deals.
- Relevant CCTV recordings.

29.2. The objective of keeping said records is to ensure that SR BULLION can provide the basic information for the reconstruction or arrangement of individual transactions, facilitate data analysis, enable the tracing of financial transactions, and, where appropriate, provide evidence for

prosecution against criminal activity.

29.3. Documents may be retained as originals or copies, or as scanned images onto pen drives, hard discs, online systems, cloud-based systems, etc., provided that such forms are admissible in the UAE Court of Law.

29.4. SR BULLION shall designate at least two (2) persons responsible for the safekeeping of records.

29.5. All records must be available for prompt and swift access by the relevant authorities when required. The request for such records by government authorities may be fulfilled within a reasonable time frame, not to exceed fifteen (15) business days.

30. RECORD RETENTION POLICY

30.1. The following document retention periods shall be followed:

- The Company will keep all customer-related records for at least five (5) years. This includes documents collected during Customer Due Diligence (CDD), monitoring records, account files, emails or communications with the customer, copies of ID documents, any suspicious transaction reports (STRs), internal analysis, relevant CCTV recording, and any other information related to AML/CFT/CPF compliance.
- The five-year period will be counted from the latest relevant event — such as when the customer relationship ends, an account is closed, a one-off transaction is completed, a regulatory inspection or investigation finishes, or a final court judgment is issued.
- If the records relate to ongoing investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed by the FIU that the case has been closed.

END OF DOCUMENT

SR BULLION FZCO

VERSION CONTROL 5.0 16.02.2026	NAME	SIGNATURE
Document Prepared & reviewed by:	**Ms. Anam Tayyaba, MLRO & Compliance Officer, SR Bullion FZCO** (Manager - Compliance, Risk & Governance, AKW Consultants, Dubai, UAE)	Anam Tayyaba
Document Approved by:	**Mr. Shitiz Garg, Owner & Managing Director, SR Bullion FZCO**	SSHITIZ

SR BULLION FZCO

APPENDIX A – NATURAL PERSON (INDIVIDUAL) KYC DOCUMENTS CHECKLIST		
	Document / Information	Completed
1	Basic Customer Information:	
	• Legal name	☐ Yes ☐ No ☐ N/A
	• Date of Birth	☐ Yes ☐ No ☐ N/A
	• Place of Birth	☐ Yes ☐ No ☐ N/A
	• Nationality	☐ Yes ☐ No ☐ N/A
2	Identity Documents:	
	• Passport	☐ Yes ☐ No ☐ N/A
	• National ID	☐ Yes ☐ No ☐ N/A
	• Visa for the Country of Residence (if applicable)	☐ Yes ☐ No ☐ N/A
3	Address Proof Documents (anyone)	
	• Utility bill (e.g., electricity, water, phone)	☐ Yes ☐ No ☐ N/A
	• Tenancy contract/purchase agreement	☐ Yes ☐ No ☐ N/A
	• Local authority tax bill	☐ Yes ☐ No ☐ N/A
4	Contact details:	
	• Telephone number(s)	☐ Yes ☐ No ☐ N/A
	• Mobile number (s)	☐ Yes ☐ No ☐ N/A
	• Email address	☐ Yes ☐ No ☐ N/A
5	Verification of contact details above via the due diligence conducted by SR BULLION staff.	☐ Yes ☐ No ☐ N/A
6	Ultimate Beneficiary Owner Declaration	☐ Yes ☐ No ☐ N/A

7	Understanding the source of funds of each Individual/ Shareholders/Ultimate Beneficiary Owner/Key Managerial People	☐ Yes ☐ No ☐ N/A
8	Whether the individual/shareholder/manager is a Politically Exposed Person (PEP) or a Close Associate of a PEP	☐ Yes ☐ No ☐ N/A
9	In case of a salaried person:	
	• Proof of Employment	☐ Yes ☐ No ☐ N/A
	• Proof of Salary	☐ Yes ☐ No ☐ N/A
10	In case of a businessman:	
	• Names and addresses of all businesses, where the customer has a stake above 25%	☐ Yes ☐ No ☐ N/A
	• License copy of all businesses	☐ Yes ☐ No ☐ N/A
	• Main products or services	☐ Yes ☐ No ☐ N/A
	• Names and addresses of other partners/owners in the businesses	☐ Yes ☐ No ☐ N/A
	• Main activities in geographical areas	☐ Yes ☐ No ☐ N/A

SR BULLION FZCO

APPENDIX B – LEGAL PERSON (CORPORATE) KYC DOCUMENTS CHECKLIST		
	Document / Information	Completed
1	Proof of legal existence of the Company:	
	• Trade License	☐ Yes ☐ No ☐ N/A
	• Certificate of Incorporation	☐ Yes ☐ No ☐ N/A
	• Share Certificates / Shareholders Register	☐ Yes ☐ No ☐ N/A
	• Memorandum of Association	☐ Yes ☐ No ☐ N/A
	• Articles of Association	☐ Yes ☐ No ☐ N/A
	• Tax Registration Certificate	☐ Yes ☐ No ☐ N/A
2	Proof of the company's Registered Address and Office/Principal Address (primary address where the business activity is performed) in the country of origin and/or physical address within the UAE:	
	• Utility bill (e.g., electricity, water, phone)	☐ Yes ☐ No ☐ N/A
	• Tenancy contract/purchase agreement	☐ Yes ☐ No ☐ N/A
	• Local authority tax bill	☐ Yes ☐ No ☐ N/A
3	Contact details:	
	• Office telephone number(s)	☐ Yes ☐ No ☐ N/A
	• Company email address	☐ Yes ☐ No ☐ N/A
	• Company website	☐ Yes ☐ No ☐ N/A
	• Key Contact mobile number	☐ Yes ☐ No ☐ N/A
	• Key Contact email address	☐ Yes ☐ No ☐ N/A
4	Verification of contact details above via the due diligence conducted by SR BULLION staff.	☐ Yes ☐ No ☐ N/A
5	Ultimate Beneficiary Owner Declaration	☐ Yes ☐ No ☐ N/A
6	Board Resolution	☐ Yes ☐ No ☐ N/A

7	Authorised Traders List (with their specimen signature)	☐ Yes ☐ No ☐ N/A
8	For all Shareholders / Ultimate Beneficiary Owner / Key Managerial People / Authorised Signatories / Power of Attorney Holders:	
	• Passport	☐ Yes ☐ No ☐ N/A
	• National ID	☐ Yes ☐ No ☐ N/A
	• Visa for the Country of Residence (if applicable)	☐ Yes ☐ No ☐ N/A
	• Address Proof	☐ Yes ☐ No ☐ N/A
9	Financial Information:	
	• Latest Audited Financial Statement (last two years)	☐ Yes ☐ No ☐ N/A
	• Latest Tax Returns	☐ Yes ☐ No ☐ N/A
10	Compliance Policies (if available):	
	• AML/CFT/CPF policies and procedures	☐ Yes ☐ No ☐ N/A
	• Responsible Supply Chain Policy	☐ Yes ☐ No ☐ N/A
	• Anti-bribery and Corruption Policy	☐ Yes ☐ No ☐ N/A
	• Whistleblower Policy	☐ Yes ☐ No ☐ N/A
11	Details of the company's business including	
	• Main products or services	☐ Yes ☐ No ☐ N/A
	• Names and addresses of parent company and/or subsidiaries, if applicable	☐ Yes ☐ No ☐ N/A
	• Main activities geographical areas	☐ Yes ☐ No ☐ N/A
12	Understanding the source of funds originating from the Company	☐ Yes ☐ No ☐ N/A