

PREVENTION OF LAUNDERING PROCEEDS OF CRIME AND COUNTERING THE FINANCING OF TERRORISM POLICY

1. INTRODUCTION

As per the regulations issued by the Financial Action Task Force (FATF1), which was established to prevent laundering proceeds of crime and financing of terrorism at an international level, member countries are now obliged to comply with these regulations and principles. MASAK (Financial Crimes Investigation Board) established by the Republic of Turkey Ministry of Treasury and Finance draws up legal regulations and carries out activities to ensure that Turkey, also a member of FATF, complies with such international regulations.

NMGlobal Kıymetli Madenler Ticaret A.Ş. (“NMGlobal” or the “Company”) adopts a policy based on the prevention of money laundering and the combating of the financing of terrorism, and, as a member of Borsa Istanbul, conducts its activities in accordance with the procedures and principles set out in the Borsa Istanbul Responsible Supply Chain Guide for Precious Metals and other applicable legislation.

In this context, NMGlobal undertakes to carry out its activities in accordance with the regulations introduced by;

- The Turkish Criminal Code no. 5237,
- Law no. 5549 on Prevention of Laundering Proceeds of Crime,
- The Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism (hereinafter referred to as “Regulation on Measures”).
- Regulation on the Program of Compliance with Obligations for the Prevention of Laundering of Proceeds of Crime and Financing of Terrorism (hereinafter “Compliance Regulation”)
- Law no. 6415 on the Prevention of the Financing of Terrorism
- Law no. 7262 on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction
- Precious Metals Responsible Supply Chain Compliance Guidelines
- Regulation on the Postponement of Transactions within the Scope of the Prevention of Money Laundering and the Financing of Terrorism
- Miscellaneous legislation as well as recommendations, principles, standards, guidelines, declarations etc. of national and international organizations, provided that they are not in conflict with the applicable legislation.

The Resolution no. 1373 (2001) of the Security Council of the United Nations, which was adopted on 28.09.2011, requires such matters that financing of terrorism be treated as a crime requiring heavy punishment, that all assets and economic resources belonging to terrorists and members of terrorist organizations be frozen without delay, that member countries work together under strong cooperation to combat terrorism, that they freeze assets of persons and entities that are reported by other members to be connected with terrorism and financing of terrorism, and that creation, whether directly or indirectly, of financial resources for terrorists and terrorist organizations be prevented. The Company complies with the regulations by avoiding engaging in any transaction with designated persons or entities in accordance with this resolution of the Security Council of the United Nations which is binding on member countries.

NMglobal is compatible with the decisions and practices of Borsa Istanbul and governmental authority at every stage of gold and silver buying and selling transactions. To be compliant, additionally, adopt the LBMA Responsible Gold and Silver Guidelines and OECD Due Diligence Guidance on Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas.

The Company commits to not enter any business relationship with any natural and/or legal person who is involved in the laundering of proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction.

2. DEFINITIONS

Money Laundering Crime: Refers to the crime set out in article 282 of the Turkish Criminal Code no. 5237 dated 26.09.2004.

The Ministry: Refers to the Ministry of Treasury and Finance.

FATF: Refers to the Financial Action Task Force (FATF), an international organization established to combat the laundering of proceeds of crime and financing of terrorism. Turkey is a member of this organization.

Beneficial Owner: Refers to natural persons who carry out a transaction within an obliged party; natural persons on whose behalf a transaction is being conducted or the natural person(s) who ultimately control(s) or own(s) legal persons, or unincorporated organizations.

Service Risk: Refers to the risks to which the Company may be exposed in connection with systems that can conduct transactions in a non- face-to-face manner via new and developing technologies, business relationships the purpose of which are not sufficiently known, and other customers, businesses, and transactions that require special handling.

Postponing Transaction: Refers to suspending a transaction or not permitting it to be conducted.

Assets: Refers to money, any kind of movable or immovable, tangible or intangible goods or rights which have monetary value, and any kind of legal documents or instruments certifying rights on them.

Freezing of Assets: Refers to removing or restricting the power of disposition on assets in order to prevent assets from being terminated, consumed, converted, transferred or assigned or put through other transactions.

Financial Crimes Investigation Board (MASAK): Refers to the board which is authorized and tasked to combat laundering of proceeds of crime. MASAK is affiliated to the Ministry (MASAK) of Treasury and Finance.

Legislation: Refers to the regulations listed in the “Introduction” section of this Policy and other relevant Regulations and Communiqués, MASAK’s resolutions and directions, and international conventions and legal regulations to which the Republic of Türkiye is a signatory.

Customer: Refers to any customer, supplier, ultimate beneficial owners, and/or right holders which are engaged in a business relationship with the Company.

Customer Risk: Refers to the risk of the Company being abused as a result of the customer’s line of business involving a lot of movements of cash or trade of high-value products/goods or allowing international fund transfers to be performed easily, or the customer or its agents or representatives involving in the laundering

of proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction.

“Know Your Customer” Principle: Refers to the activities performed, especially during the customer acceptance process, to verify the identity of customers, and to principle classify customers under specific risk categories (e.g. low, medium, high risk) and to establish customer acceptance processes accordingly by taking into account the transactions performed and the services/products used as per the parameters to be determined by the Company.

Policy: Refers to the Policy on Combating Laundering Proceeds of Crime and Financing of Terrorism

Risk: Refers to the possibility of financial loss or loss of reputation that the Company or its employees may incur due to the use of the services and operations carried out by the Company in laundering proceeds of crime or financing of terrorism or due to failure to fully comply with the legislation.

Politically Exposed Person (PEP): According to the definition provided by FATF, PEP refers to Person (PEP) individuals who are or have been entrusted with prominent public functions by a foreign country, for example heads of state or heads of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials; individuals that are entrusted with a key function at an international organization or individuals who have a function which is equivalent to those of members of senior management at such organizations and their immediate family members, including blood relatives and relatives by marriage or other similar relationship (civil partnership) or close associates of PEPs.

Proceeds of Crime: Refers to the assets obtained as a result of any crime.

Laundering of Proceeds of Crime(Money Laundering): Transactions, whereby those earnings raised from unlawful means, are injected into the financial system so as to convert them into non-cash form in particular to create the impression that they are derived from legal means, and to make them pass through a process in the financial system so as to conceal the illegal origins of the funds.

Company: Refers to NMGlobal Rafineri Sanayi ve Ticaret Anonim Şirketi

Suspicious Transaction: Refers to presence of any information, suspicion or any factor which would trigger suspicion about the fact that the assets subject to a transaction performed or attempted to be performed with or through the agency of the Company have been obtained illegally or are used for unlawful purposes or are used by any terrorist organizations, terrorists or financiers of terrorism within such scope, or are related or associated with them.

Continuous Business Relationship: Refers to a business relationship that is established between the obliged party and its customers through services.

Internal Procedures: Refers to the regulations or directions which will be implemented as per, and detailed in, the Company Policy on Prevention of Laundering Proceeds of Crime and announced across the entire Company.

Financing of Terrorism: Refers to the provision and collection of money or any goods, rights, receivables or revenues which hold monetary value and benefits and values resulting from them being converted into each other while it is known that such money or assets will be partially or completely used for committing crimes of terror.

Compliance Unit: Refers to the unit which reports to the compliance officer and consists of employees who are tasked to carry out compliance programme.

Compliance Officer: Refers to the officer assigned by the Board of Directors who is vested the required authority for ensuring compliance with obligations introduced by the law and legislation effected based on the law.

Compliance Programme: Refers to the collection of actions taken by the Company within the framework of the Company policies and procedures concerning prevention of laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction as well as the applicable legislation.

Country Risk (High-Risk Jurisdictions): Refers to the risk to which the Company may be exposed when the Company engages in business relationships and transactions with the citizens, companies and financial institutions of the countries that are announced by the Ministry out of those countries that lack sufficient regulations on prevention of laundering of proceeds of crime financing of terrorism, do not provide sufficient cooperation in the combat against these crimes or are identified as high-risk countries by authorized international organizations.

Senior Management: Company Board of Directors and/or General Manager

Obligated Party: Organizations who are obliged to fulfill the obligations (identification, reporting suspicious transactions, etc.) set out as preventive measures in the combat against the laundering of proceeds of crime.

Obligations: Regarding Prevention of Laundering Proceeds of Crime No. 5549 Envisaged within the scope of the law and other regulations; know your customer, suspicious transaction reporting, providing information and documents, obligation to preserve and present.

3. PURPOSE

To enable the Company to comply with the law, regulations, and other arrangements mentioned above and fulfill its obligations, this Policy is intended to ensure that the Company:

- (i) complies with the Law and the regulations issued by organizations authorized under the Law
- (ii) prevents use of the Company's operations for the purposes of laundering of proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction.
- (iii) conducts an assessment of the customers/suppliers and transactions with a risk- based approach in order to eliminate the risks that the Company may otherwise be exposed to
- (iv) identifies the strategies, internal controls, and measures, operating rules and responsibilities for reducing the risks which the Company may be exposed to
- (v) informs the Company employees about their obligations concerning the combat against the laundering of proceeds of crime and their legal and administrative obligations

- (vi) carries out assurance and consulting activities within the scope of the internal audit
- (vii) planning, execution, and reporting of training activities

4. SCOPE

The compliance programme to be determined and carried out with a risk-based approach to ensure compliance with the Law and the regulations and communiqués issued under the Law for the purposes of prevention of laundering of proceeds of crime and financing of terrorism include the following actions:

1. Developing corporate policies and procedures
2. Performing risk management activities
3. Performing monitoring and control activities
4. Assigning a compliance officer and establishing a compliance department
5. Performing training activities
6. Performing internal audit activities

5. AUTHORITY AND RESPONSIBILITIES

The Company managers and employees from all levels and the representatives, commercial agents and affiliates of the Company are required to fulfill all of their duties and responsibilities in an effective, proper and careful manner in order to ensure that the Company is not exposed to risks associated with prevention of laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction. The provisions of Personnel Regulation are reserved.

The Company's Board of Directors is solely responsible for executing the compliance programme in an adequate and effective manner according to this Policy.

5.1. Board of Directors

Board of Directors have the following authorizations and responsibilities concerning the compliance programme:

- (i) To ensure that the Company fulfills its obligations regarding prevention of laundering of proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction
- (ii) To assign a duly authorized compliance officer
- (iii) To clearly set out the duties and responsibilities of the compliance officer and compliance department in writing.
- (iv) To approve the Company's policies, written procedures, annual training programs and any changes to be made in them.
- (v) To evaluate the outcomes of the risk management, monitoring, control and internal audit activities to be carried out as part of the compliance programme, (vi) To take timely measures to ensure that the Company is not exposed to risks related to money laundering, financing of terrorism and proliferation of weapons of mass destruction,
- (vi) Ensuring the correct and effective execution of the works and procedures that must be implemented by all employees,
- (vii) To take actions as necessary in order to correct identified issues and deficiencies in a timely manner, and to ensure effective and coordinated execution of all compliance programmes.

(viii) To cooperate and share information with national and international regulatory authorities, where legally permissible.

5.2. Compliance Officer

Compliance officer who has the qualifications specified in the regulation and is given the necessary authorization powers by the Board of Directors; shall act bona fide in an objective and independent will, acceptable and honest manner.

The duties and responsibilities of the compliance officer are as follows;

- (i) The compliance officer assigned by the Board of Directors is required to act in good faith with integrity and in a reasonable, objective and independent manner while fulfilling their duties and responsibilities. Duties and responsibilities of the compliance officer are as follows:
- (ii) To establish communication and ensure coordination with MASAK as needed
- (iii) To coordinate and supervise development of the Company's policies and procedures
- (iv) Performing risk management and monitoring and control activities according to the Company's policies and procedures
- (v) To obtain information and findings about potentially suspicious transactions by investigating them as necessary within their authorities and capabilities and to report those transactions which they reasonably believe to be suspicious to MASAK.
- (vi) To submit activities related to training programs to the senior management for approval, and to ensure effective execution of the approved training programs.

NMGGlobal's obligation to provide information and documents to MASAK is fulfilled through the compliance officer.

The Compliance Officer is vested with the authority concerning the submission of the aforementioned matters to the Board of Directors and shall be directly accountable to the Board of Directors.

6. KNOW YOUR CUSTOMER

NMGGlobal's customer acceptance process, which is intended to help efforts to prevent laundering of proceeds of crime and financing of terrorism, is based on the "Know Your Customer" principle. The "Know Your Customer" principle plays a key role in protecting the Company from persons and actions that could be associated with money laundering and financing of terrorism. An appropriate policy which is aligned to relevant international standards and applicable legislation is devised and enforced.

Information and documentation provided are examined and reviewed to verify the identity of natural and legal persons and their representatives, the workplace and field of activity of the customer as well as the purpose and nature of the transactions and to recognize the beneficial owner. When establishing a continuous business relationship, information is obtained about the purpose of the business relationship. For the purposes of monitoring customers and transactions, up-to-date information such as the occupation, work history, activities, financial status, accounts, transactions and country of residence/operation of the customer is taken into account, and a customer profile is created. The details regarding how the customer identification process is to be conducted are outlined in the NMGGlobal Internal Control and Risk Assessment Directive

In transactions with the customer, it is necessary to obtain the relevant information and confirm the accuracy of this information with documents in order to identify the customer and reveal the real beneficiary before the transaction is carried out, as stated in the legislation and company procedure. In the establishment of a continuous business relationship, information is also obtained about the purpose and nature of the business relationship. Within the framework of the risk-based approach, the necessary information and documents are requested to obtain additional information about the customer, and additional information is requested about the asset subject to the transaction and the source of the customer's funds. Necessary reviews are made regarding the consistency of all information and documents provided during the know your customer process. In addition, within the scope of monitoring the status and transactions of customers; The know your customer process is carried out by ensuring that information about the customers' profession, business history, commercial activities, financial situation, risk profile, accounts and transactions, country of residence or operation and similar information are kept up to date.

Where the Company cannot verify the identity of a customer or obtain sufficient information about the purpose of the business relationship, the Company will not perform the transactions requested by the customer or establish a business relationship. The Company will not establish a business relationship with anonymous names and/or persons whose beneficial owner cannot be identified.

The Company will not, directly or indirectly, enter into a business relationship with those countries / regions / persons / organizations that are subject to any sanctions enforced as per the resolutions of the United Nations Security Council, sanctions issued by the European Union, the United Kingdom Treasury, OFAC sanctions issued by the United States of America Department of Treasury, sanctions issued by legal and administrative authorities in Turkey as well as other sanctions which are binding for the Precious Metals Market or that are included in the FATF's list of "Call for Action" countries and/or included in countries' blacklists related to laundering of proceeds of crime and financing of terrorism.

7. MONITORING AND CONTROL

The purpose of monitoring and control is to protect responsible persons against risks and to continuously monitor and control whether they carry out their activities according to the Law and the regulations and communiqués issued under the Law as well as corporate policies and procedures and risk assessment guidelines.

Monitoring and control activities over customer transactions are monitored, evaluated and executed as a whole within the compliance department, under the supervision and coordination of the compliance officer, by employing a risk-based approach.

As part of its continuous business relationships, the Company continuously monitors the transactions performed by its customers to ascertain that their transactions match the customer profile, and keeps up-to-date information, documents and records about its customers.

Monitoring and control activities include the following as a minimum:

- a. Monitoring and controlling the customers and transactions in the high-risk group
- b. Monitoring and controlling the transactions performed with high-risk countries
- c. Monitoring and controlling complex and unusual transactions
- d. Monitoring and controlling the transactions exceeding an amount to be determined by the Company according to the risk policy are compatible with the customer profile,
- e. Monitoring and control of linked transactions that, taken together, exceed the amount requiring identification

f. Monitoring and controlling the information and documents that must be kept in electronic environment or in writing about the customers and the information required to be included in the electronic transfer messages and completing the deficiencies and updating them,

g. Monitoring whether the transactions performed by a customer matches with the information about the customer's field of activity, risk profile and fund resources on a continuing basis.

Monitoring and control activity reports are issued periodically or upon detection of a suspicious transaction.

8. RISK MANAGEMENT

Risk management activities are intended to identify, quantify, rate, assess, mitigate, monitor, prevent, avoid or eliminate the risks to which the Company may be exposed in the context of laundering of proceeds of crime and financing of terrorism.

8.1. Accordingly, risk management activities include the following as a minimum:

- a. Developing risk identification, rating, classification, and assessment methods based on customer and country risk
- b. The grading and classification of services/products, transactions, and customers according to risks.
- c. Ensuring that risky customers, transactions or services are monitored and controlled, and taking necessary measures to reduce risks; Reporting to alert relevant units; Developing appropriate operating and control rules to ensure that the transaction is carried out with the approval of the Board of Directors and inspected when necessary.
- d. Challenging the consistency and effectiveness of risk identification, assessment, rating and classification methods retrospectively through case studies or previous transactions, and reviewing and updating the methods based on the outcomes and changing circumstances
- e. Making necessary improvements in the risk management methods and processes by monitoring the national legislation and the recommendations, principles, standards and guidelines of international organizations as applicable to the Company's risks
- f. Reporting results of risk monitoring and assessment activities to the Board of Directors on a regular basis

8.2. During risk assessment, the presence of the following is considered as high risk:

- Countries that do not have sufficient regulations concerning prevention of laundering of proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction
- Overseas centers which offer banking secrecy, tax benefits and legal immunity and thus present an attractive means to hid the proceeds of organized crime or funds used in financing terrorism (Offshore, free zones and other similar financial centers)
- Legal entities with a "Politically Exposed Person" as their ultimate beneficial owner and/or in their senior management
- Complex and unusually large transactions, or transactions and requests that customers want to perform by using newly emerging technological means and methods
- Transactions without a reasonable legal and economic purpose (which cannot be adequately justified)
- Transactions and requests of a customer which cannot be associated with the customers' previous transactions and field of activity
- Industries and occupations which involve a lot of movements of cash or trade of high-value products/goods or allow international fund transfers to be performed easily.

8.3. In order to mitigate a risk to be assumed when working with customer groups that are given a high-risk

rating, additional measures are taken in proportion to the identified risk as per our company directive. One or more or all of the additional measures can be implemented. If a risk cannot be eliminated despite additional measures aimed at mitigating the risk, no business relationship is established and any existing business relationship is discontinued. Board of Directors approval is required for entering into a business relationship, maintaining an existing business relationship or executing a transaction.

9. DETECTING AND REPORTING SUSPICIOUS TRANSACTIONS

When there is any information or suspicion or any other consideration which would require suspicion about the fact that the assets subject to a transaction, performed or attempted to be performed with or through the agency of the Company, have been obtained illegally or are used for unlawful purposes or are related or associated with them, necessary investigations are conducted. If the transaction is concluded to be suspicious, the compliance officer serves a “suspicious transaction notification” to MASAK within the timeframe and according to the principles set out in the legislation.

All parties that have information about this subject take maximum care to ensure confidentiality and security of the suspicious transaction notifications and internal notifications within the Company according to the legislation. The Company employees can submit their feedback or voice their concerns without being under the threat of any retaliation, victimization or harm.

10. TRAINING

Training activities are carried out to educate all relevant employees about their legal and administrative obligations in the combat against laundering of proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction, to ensure they fulfill their obligations, to raise awareness about the Company policy and risk-based approach, to update information and to establish the Company culture according to the applicable legislation and this Policy.

A training program is developed by the Compliance Officer. The Compliance Officer supervises effective execution of the training program. Required information and statistics are kept about the training activities as per the legislation.

11. INTERNAL AUDIT

The function of the internal audit is to provide assurance to the board of directors about the effectiveness and adequacy of compliance programme. Internal audit activities contain annually and on a risk-based approach, examination and controlling of institutional policy and procedures, risk management, monitoring and controlling activities and whether the training activities are sufficient and efficient, sufficiency and efficiency of risk policy of obliged party, whether the transactions are carried out in compliance with Law and regulation and communiques issued in accordance with Law and institutional policy and procedures.

When determining the scope of audits, the related business, transaction volumes, deficiencies detected during monitoring and control activities, and risky customers, services and transactions are taken into account. Any identified deficiencies, errors and abuses as well as opinions and recommendations for preventing re-occurrence of such deficiencies, errors and abuses are reported to the Senior Management.

The internal audit provides assurance to senior management that transactions are monitored and audited with a risk-based approach to determine whether they are carried out according to the legislation, the Company Policy and procedures.

12. OTHER OBLIGATIONS UNDER THE REGULATIONS CONCERNING FINANCING OF TERRORISM AND FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

The Company complies with the Law no. 6415 on the Prevention of the Financing of Terrorism (“Law no. 6415”) and the Law no. 7262 on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction (“Law no. 7262”) as well as any regulations issued under these laws. Therefore, the Company adheres to any decision issued by MASAK on the freezing of assets.

Upon receiving a notification from MASAK, the Company notifies MASAK accordingly. If the Company does not have control over the related assets or have records of the related assets, it notifies MASAK about this information. If the Company has control over the related assets or has records of the related assets, it freezes the assets in question and notifies MASAK by stating that the assets have been frozen and providing the details of the assets frozen. In either case, the Company will deliver the notification to MASAK via the same method of delivery no later than seven days after receiving the notification. If the freezing decision is canceled, the Company will notify MASAK that action has been taken according to this decision by following the same principles and procedures described above. The right of disposal on any assets for which a freezing decision is taken can only be exercised with the permission of MASAK. Any person whose assets have been frozen may not terminate, consume, convert, transfer or assign such assets or perform other transactions on the assets unless permitted by MASAK. The Company may not perform or facilitate such transactions.

13. MAINTAINING RECORDS AND CONFIDENTIALITY OF RECORDS

As per the applicable legislation in force in Turkey, any information, document and record that need to be obtained and maintained about customers and transactions will be stored in a database for eight (8) years in a readily accessible manner by taking the required measures set out in the applicable legislation.

14. FEEDBACK FROM STAKEHOLDERS

We value and pay attention to any feedback and opinions of related stakeholders about this Policy. Feedback on, and/or violations of, this Policy can be communicated through any of the following channels. We comply with the personal data protection laws when handling such feedback.

E-mail : etik@nmglobal.com.tr

Address : İkitelli OSB Mah. Atatürk Bulvarı No:114, İç Kapı No:236 Başakşehir İstanbul/Türkiye

Phone : +90 212 603 09 68

15. EFFECTIVE DATE

The updating of this Policy, when necessary, falls under the authority and responsibility of the Board of Directors. Any updates to the Policy are carried out by the Compliance Department with the support of the Legal Department and submitted for the approval of the Board of Directors.

This Policy has been approved by the Board of Directors and entered into force on 01.10.2025.

Date of Board of Directors' Decision	Version No.
06.04.2020	(1)
10.04.2020	(2)
28.06.2021	(3)
01.11.2022	(4)
17.07.2023	(5)
01.10.2025	(6)