



Cengiz Holding A.Ş.

Anti-Money Laundering and Counter-Terrorist Financing Policy ("AML / CTF Policy")

Table of Contents

1. Purpose and Scope 3

2. Definitions 3

3. General Principles 4

4. Implementation Principles 4

5. Training and Awareness..... 6

6. Roles and Responsibilities 6

7. Revision History 6

1. Purpose and Scope

This Anti-Money Laundering and Counter-Terrorist Financing Policy (“Policy”) has been prepared to set forth the principles, rules, and methods adopted by Cengiz Holding A.Ş. and its Group Companies (“Cengiz Holding”, “Holding” or “Group”) in order to ensure full compliance with national and international regulations and to prevent money laundering and the financing of terrorism.

This Policy is prepared in line with the 40 Recommendations published by the Financial Action Task Force (FATF), as well as other laws and regulations issued in Türkiye regarding the prevention of money laundering and the financing of terrorism, with the aim of guiding employees.

The Policy applies to all geographies in which the Holding operates, covering all commercial and financial transactions carried out with employees, customers, business partners, and other third parties. Within this framework, risk-based controls to be implemented before and during the business relationship, the retention of required records, suspicious transaction reporting, and compliance trainings fall within the scope of this Policy.

2. Definitions

Unless otherwise defined under this Policy, the terms, words, and expressions used herein shall have the meanings ascribed to them under applicable laws, regulations, and sectoral practices.

Due Diligence: Refers to the process of identifying third parties of the organisation and verifying such identification through reliable sources, determining the ultimate beneficial owners in financial transactions, obtaining shareholding information in legal entities, identifying the persons to whom ownership belongs, gathering information on the type and nature of the intended transaction, and applying all these processes periodically after the business relationship has been established.

Financial Action Task Force (FATF): An organisation established in 1989 with the aim of preventing money laundering and the financing of terrorism.

Ultimate Beneficial Owner (UBO): The natural person(s) who ultimately own or control a business and/or on whose behalf a transaction is conducted.

Money Laundering: The process of disguising illegally obtained proceeds as legitimate funds and integrating them into the financial system.

Politically Exposed Person (PEP): Persons who hold prominent public functions. PEPs include, but are not limited to, the following:

- Heads of state or government, ministers, and deputy ministers,
- Members of parliament,
- Judges of supreme courts, constitutional courts, or other high-level judicial bodies,
- Ambassadors,
- Members of central bank boards,
- Senior military officers,
- Members of administrative, management, or supervisory bodies of state-owned enterprises,

- Persons performing equivalent functions, as well as all their family members and close business associates.

Terrorist Financing: The provision of financial resources to individuals or organisations that support terrorist activities.

Third Party: Any supplier, contractor, subcontractor, dealer, distributor, intermediary, or any representative or consultant acting on behalf of or for the account of the Holding.

Office of Foreign Assets Control (OFAC): A department of the U.S. Department of the Treasury responsible for the implementation and administration of U.S. economic sanctions and the imposition of administrative penalties under such sanctions.

Sanctions and Prohibited Lists: Lists issued by the United Nations, European Union, the United States, and other national or international authorities identifying countries, entities, or individuals subject to trade restrictions or prohibitions.

Suspicious Transaction: Any transaction lacking a reasonable legal or economic basis, deviating from the normal transaction profile, or raising suspicion of money laundering or terrorist financing.

3. General Principles

Money laundering is classified among crimes subject to severe sanctions under national and international regulations. In this context, Cengiz Holding diligently monitors and complies with all applicable laws and regulations in both its domestic and international operations to prevent money laundering and the financing of terrorism.

Cengiz Holding adopts a risk-based approach in its business relationships with third parties; in this regard, it conducts due diligence and identity verification checks, implementing necessary preventive measures both prior to and throughout the course of the business relationship. Periodic reviews are carried out on ongoing business partners to ensure the early detection of potential non-compliance related to money laundering and terrorist financing.

In these processes, Cengiz Holding ensures adherence to national and international standards, including the FATF Recommendations, MASAK regulations, and EU and U.S. sanctions regimes. This approach not only ensures compliance with the law but is also of critical importance for the Holding's reputation, financial sustainability, and stakeholder trust.

4. Implementation Principles

Cengiz Holding conducts due diligence on third parties before entering into and throughout the course of business relationships to determine whether such parties are connected to money laundering or the financing of terrorism.

In this context, the following processes must be implemented for third parties:

- Identification of the ultimate beneficial owners and authorised signatories of individual and corporate customers, suppliers, business partners, and other third parties, along with adverse media screening and checks against sanctions lists. For corporate identification, information must include the legal entity's name, trade registry number, tax identification number, business activity, full address, telephone number, email address, and the details of the authorised representative (full name, place and date of birth,

nationality, type and number of ID document, and specimen signature). For Turkish citizens, the Turkish Republic ID number must also be collected. Verification of the corporate entity's name, trade registry number, business activity, and address must be carried out through trade registry documents; verification of the tax ID number through documents issued by the Turkish Revenue Administration; and verification of the identity of authorised persons through ID cards, driver's licences, or passports for Turkish nationals, and passports or residence permits for non-Turkish nationals. All information and documents obtained must be retained for submission to the relevant authorities in case of irregularities.

- Detailed information must be obtained regarding the purpose of goods purchased in commercial transactions with third parties.
- Customers, suppliers, and other third parties must be subject to periodic monitoring and reviews, based on the results of the pre-contractual risk assessment. This risk assessment must be conducted using the outputs of the due diligence process. In line with the information gathered, a third party must be considered high-risk if: it operates in high-risk countries or regions; its ultimate beneficial owners include politically exposed persons (PEPs); it engages in or seeks to establish relationships involving significant cash transactions; it is subject to adverse media; or it appears on international sanctions lists.
- The Human Resources Department must conduct sanctions screening and adverse media checks for employees and candidates applying for managerial and higher-level positions. If an adverse finding arises, the matter must be referred to the Legal Department, which, after its assessment, will escalate the case to the Board of Directors for a final decision. The results of all checks must be documented and retained.
- Necessary checks for customers and third parties must be carried out by the process owner. If any adverse findings arise, the matter must be reported to the Legal Department. After evaluation, the Legal Department will provide its recommendation to the Board of Directors regarding whether to enter into or continue the business relationship. The process will be finalised in line with the Board's decision, under the coordination of the Legal Department.

Examples of adverse situations that may arise during the controls include:

- Inconsistencies in the information obtained from the parties prior to contract signing,
- Reluctance by the parties to disclose information such as ownership structure and ultimate beneficial ownership,
- The planned transaction being conducted at an unusually high value compared to normal market practices,
- Payments via bank transfer being made by unrelated third parties of unknown origin,
- Requests for unregistered or cash payments.

The Legal Department is responsible for ensuring compliance with legal regulations on the prevention of money laundering and terrorist financing, and for monitoring regulatory developments to ensure necessary controls are established. Following its assessment, the Legal Department will provide its recommendation to the process owner and the Board of Directors regarding whether to continue the business relationship. If the Board decides to proceed, the compliance risk level of the customer or supplier must be updated after the due diligence process, and the relevant party must then be monitored at closer intervals by the process owner.

The monitoring responsibility lies with the process owner, while oversight of these controls must be conducted by the Legal Department.

5. Training and Awareness

In order to ensure compliance with local and international regulations on the prevention of money laundering and to increase Cengiz Holding employees' awareness of risks within the framework of relevant policies and rules, all relevant employees must be provided with regular training. In particular, employees working in, or to be assigned to, process-owning departments that initiate business relationships with third parties are required to receive this training annually. The completion of employee training is the responsibility of managers and the Human Resources Department, while the organisation of training sessions and the monitoring of participation are carried out by the Human Resources Department.

6. Roles and Responsibilities

All Cengiz Holding employees are obliged to comply with this Policy. In the event of encountering a situation that violates the rules set forth in the Policy, employees must promptly report the matter through at least one of the following channels:

- Legal Department,
- Business Development Department
- Accounting Department
- Finance Department

The responsibility for communicating the requirements of this Policy to employees and for establishing an internal control environment that ensures employees act in compliance with the Policy lies with the Business Development, Finance, Accounting, and Legal Departments.

In countries where Cengiz Holding operates, if the legal regulations falling within the scope of this Policy are stricter than the provisions of the Policy, the relevant legal regulations shall prevail.

Employees who fail to comply with this Policy may face various disciplinary sanctions, including termination of employment.

7. Revision History

This Policy has been approved by the relevant Board of Directors Resolution of the Company and entered into force. The periodic update of the Policy in line with changes in legal regulations and Group processes is the joint responsibility of the Business Development, Finance, Accounting, and Legal Departments.

Revision No.	Revision Date	Description
01	15.09.2025	Revised to enhance alignment with applicable legislation, international standards, and company practices.