

UNICEF ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT) POLICY

Document Number : POLICY/DFAM/2022/004

Effective Date : 1 December 2022

RATIONALE

1. UNICEF operates in difficult contexts and in many cases, under extremely challenging operating circumstances. As a result, it could be exposed to the risks of money laundering and financing of terrorism. The risks may arise from fund raising activities, programme implementation, contractual arrangements, the operating environment, or from working with different Counterparties, in pursuance of the organization's mandate.
2. This policy affirms UNICEF continued commitment and its approach to combating money laundering and countering the financing of terrorism, including a reiteration of the controls and measures that UNICEF has in place in this regard.
3. The policy also outlines the principles and minimum standards of internal AML/CFT controls which should be adhered to in order to prevent abuse of UNICEF resources through money laundering (ML) or financing of terrorism (FT); mitigate reputational, regulatory, legal and financial loss risks; guard against relationships or transactions that may facilitate ML/FT; and exercise due diligence when dealing with Counterparties or persons working on behalf of or connected to Counterparties.
4. This policy is a part of a broader set of policies that are aimed at ensuring that funds mobilized to support UNICEF work are used for the purposes intended. This policy lays out a set of basic principles to guide operations and decision making.

APPLICABILITY / SCOPE

5. All UNICEF offices, personnel and Counterparties, including fundraising partners (e.g. National Committees), Implementing Partners, Suppliers and Service providers, are required to adhere to this AML/CFT policy to protect resources managed by UNICEF from being used for money laundering and financing terrorism; and ensuring responsibilities are discharged in a manner that enables the full implementation of this policy.
6. This policy complements the prevailing mandatory obligations and ethical standards applicable to the recruitment and employment of UNICEF staff, including but not limited to: United Nations Staff Regulations and Rules, [UNICEF Financial Regulations and Rules](#), Code of Conduct, [Oath of Office](#), [Standards of Conduct for the International Civil Service](#), and [UNICEF administrative issuances](#).
7. Personnel and entities, listed under paragraph 5 above, are required to be familiar with the forms in which money laundering and financing of terrorism might occur in the operating environment, and to be alert to any risk indicators or "**red flags**" that might indicate such activities (see [Annex 2](#)).
8. UNICEF shall take steps to ensure that entities with which it partners; have Regulations, Rules, Policies, and Procedures that are consistent with the principles of this policy.
9. For the purposes of this policy, relevant terms and acronyms have been defined and included in the [Annex 1](#).

POLICY STATEMENTS

10. The United Nations Security Council Resolutions have reaffirmed the United Nations call to all states to sign, ratify, and implement the relevant international conventions criminalizing terrorism and terrorist financing. The United Nations General Assembly Resolution 60/288 (2006) also encourages Member

States to implement the comprehensive international standards on combating money laundering and the financing of terrorism & proliferation recommended by the Financial Action Task Force (FATF).

11. In compliance with the United Nations Security Council sanctions regime and consistent with the Financial Action Task Force (FATF) recommendations, UNICEF does not partner with entities or individuals that participate in or support activities related to money laundering or financing of terrorism.
12. UNICEF Counterparties shall be responsible for identifying and mitigating the risks of money laundering (ML) and financing of terrorism (FT) in deploying and managing UNICEF resources.
13. UNICEF prohibits and actively prevents any activity that facilitates money laundering or the financing of terrorism. Considering its status as an independent inter-governmental organization, and in accordance with the privileges and immunities accorded to it pursuant to the United Nations Charter, UNICEF is not obligated to implement sanctions imposed by individual States or other intergovernmental organizations.
14. The Office of Internal Audit and Investigations, in accordance with its mandate, may periodically assess compliance of UNICEF offices with this policy.

POLICY ELEMENTS

15. **Money laundering** *“is the processing of criminal proceeds to disguise their illegal origin”*¹. Through this, an individual or legal entity conceals or disguises the identity or the origin of illegally obtained proceeds, for example, by concealing or disguising the fact that the source of the funds is not legitimate and that the objective is to ‘launder’ it through transactions to regain access to clean funds.
16. **Financing of terrorism** is the process by which a person or legal entity tries to collect or provide funds with the intention that they should be used to carry out a terrorist act by a terrorist or a terrorist organization as defined in the International Convention for the Suppression of the financing of terrorism as well as in any one of the treaties listed in the annex to that Convention².
17. UNICEF shall adopt a **risk-based approach** when engaging Counterparties in order to combat money laundering and financing of terrorism. This risk-based approach is the process of identifying, assessing and understanding ML/FT risks related to activities and areas where UNICEF is most exposed; and to take measures commensurate to those risks to mitigate them effectively. This approach aligns with one of the international best practices such as FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – Recommendation 1³.
18. UNICEF offices shall perform an [Annual Risk Assessment \(ARA\)](#) to assess exposure to relevant risks, including those of ML/FT, which are mandatory for all UNICEF offices.
19. To adequately manage the risk of ML/FT, UNICEF shall conduct risk-based screening of Counterparties to identify, assess and understand ML and FT risk and in accordance with the applicable due diligence protocol and requirements, before working with them as follows:

A. Due Diligence

20. UNICEF shall apply risk-based due diligence approach, informed by Counterparty type and context; to confirm, verify and validate the identity of a Counterparty and enable a reasonably informed decision regarding engaging with a party. This enables UNICEF, among other things, to assess and evaluate the extent of risk related to ML and FT regarding the relationship with the prospective Counterparty.

¹ <https://www.unodc.org/unodc/en/money-laundering/index.html>

² United Nations Office on Drugs and Crime (UNODC) / International Monetary Fund (IMF), [Model legislation on money laundering and financing of terrorism](#), December 2005, Introduction, p. 2.

³ [The FATF recommendations-International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation](#)

21. UNICEF shall seek out relevant background and business intelligence information on potential partners in order to identify and assess red flags with an aim to preventing and/or putting mitigation measures in place to protect UNICEF reputation and its investments.

B. Counterparty relationships

22. UNICEF shall take reasonable measures to duly assess the purpose, economic rationale and overall ML/FT and related integrity aspects of the Counterparty and its beneficial owners to avoid being involved in relationships that expose the organization to risk.
23. All new agreements with entities covered under the scope of this policy should include an obligation to comply with the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy.
24. UNICEF shall not engage with, and will terminate Counterparty relationships as follows:
- (a) UNICEF shall not partner with any person or entity that engages in activities inconsistent with United Nations Security Council Sanctions, and Resolutions.
 - (b) UNICEF shall not partner with Counterparties who are currently under any financial sanctions imposed by the United Nations.
 - (c) UNICEF will terminate the existing Counterparty relationship with Counterparties who do not cooperate with this policy.

C. Monitoring

25. Monitoring the status of Counterparties (not in the sanctions list) and credit quality of financial service providers (FSPs) on an ongoing basis is a key objective to ensure that UNICEF engages only with reputable and financially stable service providers and safeguarding the organization's financial assets.

D. Reporting

26. UNICEF uses the United Nations Partner Portal (UNPP) to screen Civil Society Organizations (CSOs) and their management against the UN Sanction List. UNPP has an automated continuous screening process and "red flags" any CSO with a member on the UN Sanctions list. Any suspicious information or red flag that comes to the attention of the pertinent office or partners should immediately be reported to DAPM and Office of the Comptroller for further advice. This must be done without informing or tipping off the party being reported.
27. The Head of Office or the delegated authority must seek clarification from the Office of Comptroller (Internal Controls, Compliance and Oversight Unit) regarding any partnership, contractual arrangement, transaction or activity suspected to be non-compliant with this policy.

E. Confidentiality

28. UNICEF shall ensure that all information on partners engagement, and transactions obtained in line with this policy requirement is kept confidential.

F. Record Keeping

29. Record-keeping is an essential component of the audit trail and as a result, UNICEF offices will keep all records created or obtained in relation to due diligence process and documentation regarding contractual or other arrangements with Counterparties in accordance with UNICEF [Procedure on Retention of Recorded Information](#) and the [Policy on Personal Data Protection](#).

SPECIAL CONSIDERATIONS IN EMERGENCY CONTEXTS

30. In Emergency context, the risk of inappropriate actions is much higher, and managers must be extra vigilant. If it is not practicable to carry out the required due diligence, the Comptroller's prior approval must be obtained to ensure that there are proper safeguards and that risks relating to money laundering and financing of terrorism are adequately managed.

31. TRANSITIONAL MEASURES

Not Applicable.

DOCUMENT MANAGEMENT INFORMATION PAGE

Document Title	Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy
Document Number	POLICY/DFAM/2022/004
Effective Date	1 December 2022
Mandatory Review Date	1 December 2027 This Policy shall be reviewed at such intervals as required, but no later than five years from the effective date, to reflect international best practices, consistent with evolving United Nations and FATF recommendations.
Responsible Business Owner	Office of the Comptroller, DFAM
Responsible Manager	Chief, Internal Controls, Compliance and Oversight Unit
Document Summary	This policy establishes the framework to mitigate the risk of, and combat money laundering and counter the financing of terrorism in UNICEF operations.
Regulatory content the Document Replaces	NA
Topics Covered	Anti-money laundering and countering the financing of terrorism
Corporate Risk Area	Reputation, Fraud, Waste and Misuse of Resources
Reference / Links to Enabling Legislation and Background	https://www.fatf-gafi.org/faq/moneylaundering
Links to Relevant Policy	UNICEF Policy on Financial Master Data Management Procurement policies UNICEF Supply Division UNICEF Policy on Enterprise Risk Management
Links to Relevant Procedure	UNICEF Procedure on Financial Vendor Master Data Management UNICEF Procedure on master data management of implementing partners Procedure on Retention of Recorded Information UNICEF Procedure for Risk Escalation Corporate Fundraising and Partnerships Due Diligence
Links to Relevant Guidance	UNICEF General terms and conditions of contracts Programme Cooperation Agreement United Nations Security Council Consolidated Sanctions List The FATF recommendations-International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation
Links to Relevant Training Materials	None
Links to Other Knowledge & Information Resources	UNICEF Enterprise Risk Management United Nations Global Marketplace (UNGM) UN Partner Portal - Where UN Agencies and Civil Society Partners Connect Financial Action Task Force (FATF)

ANNEX 1: TERMS and ACRONYMS

For this policy the following terms shall have the meaning set out below:

- i. **Counterparty:** Any third-party that contributes to, executes, implements, bids for, or in any way participates in UNICEF related activities, including procuring, giving or receiving of funds, services or supplies, or other form of support to or from UNICEF. Counterparties include Implementing Partners, Fundraising Partners, Supplies and Services Providers, and Financial Service Providers.
- ii. **Civil Society Organizations (CSOs):** Are non-profit, non-governmental entities designed to advance collective interests and ideas. UNICEF differentiates CSOs based on four broad categories: (a) International NGO (INGO) is an NGO that has offices in more than one country; (b) National NGO is an NGO established in only one country; (c) Community Based Organization (CBO) is a grassroots association; (d) Academic institution is a degree conferring institution.
- iii. **Due diligence:** A process to identify, verify and validate the identity of the Counterparty. This enables UNICEF to assess and evaluate the extent of risk related to money laundering and financing of terrorism regarding the relationship with the prospective Counterparty. Due diligence will be conducted by relevant UNICEF office, noting that for certain categories of Counterparties due diligence services may be centralized to a specific HQ unit, e.g., private sector corporate, foundation and philanthropy donors.
- iv. **Donor:** is a private sector entity, individual, government, intergovernmental agency or non-governmental or other organization making a monetary or in-kind contribution to UNICEF.
- v. **FATF: Financial Action Task Force** is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions with a mandate to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. FATF standards and guidance are deemed to reflect international best practices.
- vi. **Financing of terrorism:** Described as the process by which a person tries to collect or provide funds with the intention that they should be used to carry out a terrorist act by a terrorist or a terrorist organization as defined in the International Convention for the Suppression of the financing of terrorism as well as in any one of the treaties listed in the annex to that Convention⁴.
- vii. **Master Data:** Are consistent and uniform identifiers and attributes used to reference information included in lists or databases that is stored and used in UNICEF IT systems and which link all individuals and entities to financial transactions.
- viii. **Master Data Management:** Is the comprehensive method of enabling UNICEF to link all critical and financial data to a common point of reference, master data, which then facilitates UNICEF multiple systems, platforms and applications to connect together for different purposes as required by UNICEF.
- ix. **Money laundering:** The processing of criminal proceeds to disguise their illegal origin⁵. Through this, a person or legal entity conceals or disguises the identity or the origin of illegally obtained proceeds, for example by concealing or disguising the fact that the source of the funds is not

⁴ United Nations Office on Drugs and Crime (UNODC) / International Monetary Fund (IMF), [Model legislation on money laundering and financing of terrorism](#), December 2005, Introduction, p. 2.

⁵ <https://www.unodc.org/unodc/en/money-laundering/index.html>

legitimate and that the objective is to 'launder' the funds through transactions to regain access to clean funds⁶.

- x. **National Committee:** Is an independent non-governmental organization established under national law for the purposes of promoting the aims and objectives of UNICEF and advancing children's rights and well-being through resource mobilization, advocacy and other activities in its territory in accordance with agreed arrangements with UNICEF.
- xi. **Red flag:** A term used to denote a warning signal or a sign of some problem requiring attention. Money laundering and financing of terrorism usually indicate red flags before they are committed. The red flags vary depending on the type of scheme and the ability to recognize them early can help to prevent the actualization of the scheme.
- xii. **Risk:** The effect of uncertainty on objectives (an effect can be negative threat or hazard, positive or opportunity a mixture of both) (deviation from what is expected) the possibility an event will occur, or circumstance will arise that affects the achievement of objectives.
- xiii. **Risk-based approach:** The process of identifying, assessing and understanding money laundering and financing of terrorism risks to which UNICEF is exposed and adoption of appropriate measures to mitigate the risk.
- xiv. **Vendor:** Is defined as an offeror or provider (registered, actual or potential) of goods, services and/or works supplied to UNICEF. Vendor data held in UNICEF VISION is required in the day-to-day business processes related to the vendor. It includes items such as name, address, currency of payment, bank details etc. A Vendor Master Record is a data record containing this information in UNICEF VISION.

⁶ Financial Action Task Force (FATF) - <https://www.fatf-gafi.org/faq/moneylaundering>

ANNEX 2: RED FLAGS

The risk indicators below are not intended to be exhaustive but to show a few **potential** signals of money laundering and financing of terrorism activities. Red flags are not sufficient basis to confirm the existence of money laundering or financing of terrorism activity. They only trigger further review, checks and verification to be satisfied that the transaction is not contributing to money laundering or funding of terrorism, in accordance with this policy.

- a. The source of funds from a donor is suspicious - such as funds received from a high-risk entity (dubious reputation, unverified identity) or country with weak financial infrastructure, or donor with links to those that engage in or support money laundering activities or financing of terrorism, or large contributions in cash, not through the financial system.
- b. Counterparty provides false or inconsistent information during the due diligence verification – this may include fake documents, email accounts that cannot be found on the internet and so on – provision of false or suspicious information should arouse further queries.
- c. Counterparty is reluctant to provide needed information or data for due diligence verification. This could include refusal to provide details of principals or key management or those with majority interest in the entity.
- d. Counterparty is overly secretive of the entity's business or evasive regarding their clientele, beneficial owners among others.
- e. Counterparty is using an agent or intermediary without adequate or logical justification or uses email address with unusual domain part.
- f. Counterparty requests for partnership or services or transactions not compatible with those declared or not typical for that type of entity.
- g. Counterparty requests to be paid in cash instead of bank-to-bank transfer. UNICEF procedure is to pay suppliers or implementing partners through the bank system.
- h. Frequent changes of vendor's bank accounts by Counterparty without adequate justification. There are genuine reasons for changing bank accounts, however, when such request becomes frequent or urgent, special care should be taken prior to effecting the change in VISION.
- i. Multiple bank accounts belonging to the same supplier or implementing partner without good reasons.
- j. Request to pay a supplier or implementing partner through a third party. UNICEF process requires payments to be made directly to the service provider or implementing partner unless "alternate payee" has been authorized by UNICEF approving officer to that effect.
- k. Structuring transactions to avoid government reporting, tax compliance or record keeping requirements.
- l. Refunds from implementing partner using unusually complex structures that bear no connection with the implementing partners registration.
- m. Refunds of programme funds in cash – programme refunds should be done through the bank.
- n. Wire transfer activity that is not consistent with the business activities of a vendor, or which originates or terminates with parties unrelated to the transaction.
- o. An unauthorized person acting as representative or signatory of a Counterparty, or a person claiming to be a representative but not ever listed or introduced as a formal party to the transaction or relationship.