



**SAHARA
AND SAHEL
OBSERVATORY**

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM POLICY

May, 2023

TABLE OF CONTENTS

Acronyms.....	3
Definitions	4
1. Introduction and Rationale	6
2. Objectives.....	6
3. Scope	7
3.1. At the institutional level	7
3.2. At the counterparties level.....	7
4. Principles	7
5. Key provisions	7
5.1. Due diligence	7
5.2. Monitoring.....	8
5.3. Reporting.....	8
5.4. Record keeping.....	8
5.5. Implementation and obligations	8
6. Accountabilities.....	9
6.1. The Executive Secretary	9
6.2. Department Coordinators	9
6.3. External and Internal audits	9
6.4. Monitoring and Reporting Team	9
6.5. Secretariat staff	9
6.6. Other staff members, consultants and other associated persons	9
7. Effectiveness and Revision	10

ACRONYMS

AML/CFT	Anti-Money Laundering/Counter Financing of Terrorism
CDD	Counterparty Due Diligence
FATF	Financial Action Task Force
GCGHU	Governance Compliance and Grievance Handling Unit
ML	Money Laundering
MRT	Monitoring and Reporting Team
OSS	Sahara and Sahel Observatory
TF	Terrorism financing
UNODC	United Nations Office on Drugs and Crime

DEFINITIONS^{1,2,3}

Anti-money laundering (AML): A set of laws, regulations and procedures designed to prevent, detect, and report money laundering.

Beneficial Owner: Individual(s) who ultimately own or control a legal entity, and benefit from its ownership or control.

Counter Financing of Terrorism: Key component of anti-money laundering (AML) and counter-terrorism financing (CTF) efforts. It is seen as a means of destroying the ability of terrorists to carry out their activities.

Counterpart relationship: refers to the relationship between the OSS and its Counterparties.

Counterparty Due Diligence (CDD): Process which identifies and checks the true identity of the Counterpart. This would enable the Fund to assess and evaluate the extent of ML/TF risk, associated with the proposed Counterparty.

Counterparty: Any individual, organization, institution or other, involved in the OSS activities.

Covered Individuals: Any individual working at any level or grade with the OSS, who are required to comply with various obligations, such as performing CDD, reporting suspicious transactions, and maintaining adequate AML/CTF policies and procedures.

Financial Action Task Force (FATF): Intergovernmental organization established in 1989 to combat money laundering and terrorism financing. Its primary function is to develop and promote policies, standards, and measures to combat money laundering and terrorism financing. Its work is critical in the fight against money laundering and terrorism financing, given its contribution to ensuring that the international financial system is not used to facilitate such illicit activities.

Governance Compliance and Grievance Handling Unit (GCGHU): Independent body within the OSS that reports directly to the Executive Secretary. It is responsible for ensuring adherence to governance principles and regulations. It oversees the implementation of OSS' policies and procedures, and addresses grievances or complaints raised by stakeholders, partners or any individual or entity working or involved in OSS' activities. This unit plays a crucial role in promoting transparency, accountability, and ethical conduct, while effectively managing and resolving any grievances or disputes that may arise within the organization.

Money Laundering (ML): A process by which the property or income of illegal activities are transformed into seemingly legitimate funds, usually through a transaction or a series of transactions attempting to disguise their illegal source.

¹<https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf>

² <https://www.greenclimate.fund/sites/default/files/document/aml-cft-policy.pdf>

³ <file:///C:/Users/Admin/Downloads/afd-group-policy-prevent-and-combat-prohibited-practices.pdf>

Monitoring and Reporting Team (MRT): Subdivision of the Governance Compliance and Grievance Handling Unit in charge of monitoring and reporting any suspicious activity, related to money laundering and terrorism financing.

Prohibited Practices Policy: OSS' Policy on prohibited practices

Red Flag: As part of the fight against money laundering (AML) and terrorist financing (TF), the red flag is a warning signal, which alerts on the detection of suspicious behaviors, transactions or any other specific indicators. It alerts that a customer, a transaction, or any other activity, could be involved in illegal activities, including money laundering, terrorism financing, or any other illicit activity. Through the alert, the red flag helps to prevent the above-mentioned suspicious illegal behavior and activity and to protect the integrity of the financial system. To protect their operations, regulated entities are required to consider red flag alerts, and take appropriate action when suspicious behavior or activity is detected, including money laundering and terrorism financing.

Risk-based Approach (RBA): Process of identifying, assessing and understanding ML/TF risks to which the OSS is exposed, as well as the appropriate measures to mitigate them.

Terrorism Financing (TF): Provision of funds or other financial support to individuals or groups, engaged in acts of terrorism.

Terrorism: Use of violence and intimidation in the course of political or ideological goals. It is often led by non-state actors such as extremist groups, to sow terror and undermine governments or societies.

Tipping-off: Information of the Counterparty, that a suspicious transaction or related information has been disclosed to the Management or the Authorities.

1. INTRODUCTION AND RATIONALE

Combating money laundering (ML) and terrorism financing (TF) is a worldwide issue that necessitates concerted and collaborative action from a wide range of entities. An effective Anti-Money Laundering and Counter Financing Terrorism (AML/CFT) Policy is critical, as it helps comply with regulatory requirements and minimize financial and reputational risks.

The Sahara and Sahel Observatory (hereinafter referred to as "OSS" or "Observatory") is committed to complying with the highest ethical standards regarding anti-money laundering (AML) and counter financing of terrorism (CFT), in accordance with the recommendations of the Financial Action Task Force (FATF) referred to in its *"International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation"*⁴. This Anti-Money Laundering and Counter Financing Terrorism Policy (hereinafter, the "Policy" or "AML/CFTP") aims to safeguard the OSS against money laundering (ML) and the financing of terrorism (FT).

The AML/CFTP will ensure that the Observatory's resources are not used to finance any illegal act related to Money Laundering or Terrorism Financing, and also reduce financial and reputational risks. The Policy sets the threshold for AML/CFT's principles and internal control requirements that the OSS should comply with, in order to mitigate reputational, regulatory, legal and financial loss risks. The Observatory shall continuously review and update the Policy to ensure its accordance with changing regulatory requirements and international best practices. Furthermore, the Policy shall be consistent with the relevant United Nations Office on Drugs and Crime (UNODC) conventions⁵, and recommendations of the FATF⁶.

2. OBJECTIVES

The Policy implementation will prevent the misuse of the Observatory's resources for illegal purposes and enhance its ability to detect and block money laundering and terrorism financing activities.

This AML/CFTP provides the OSS with a, to guide its efforts in:

- Ensuring that the Observatory complies with legal and regulatory requirements related to AML&CFT rules, therefore, preserving its reputation. These requirements may include regulations issued by government agencies or international organizations.
- Preventing the use of the Observatory's resources for money laundering and terrorism financing activities.
- Detecting and blocking money laundering and terrorism financing activities.
- Ensuring that entities, institutions and/or individuals involved in the OSS activities comply with international AML/CFT laws and regulations.
- Conducting enhanced due diligence on high-risk stakeholders, thereby helping prevent fraudulent activities and financial crimes.

⁴ <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>

⁵ <https://www.unodc.org/unodc/index.html>

⁶ <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>

- Supporting the establishment and/or capacity building of the OSS member countries, to meet the Observatory's standards related to AML/CFT.

These objectives are achieved through supervisory activities i.e. due diligence, transaction monitoring, and suspicious activities reporting.

3. SCOPE

The AML/CFTP shall apply across two different but complementary levels:

3.1. AT THE INSTITUTIONAL LEVEL

The OSS staff, Board Of Administration members, and any other person working for the OSS, must comply with this Policy in order to protect the Observatory and its reputation from ML and/or TF abuse, thereby ensuring that they are able to perform their duties appropriately and enabling the Policy to be fully implemented.

3.2. AT THE COUNTERPARTIES LEVEL

The OSS must ensure that the executing entities or any other institution, organization or person involved in its activities comply with the Policy.

4. PRINCIPLES

The OSS commits to:

- (i) Abide by the Policy in all its activities;
- (ii) Forbid its resources to be used in any way possible for ML and/or TF purposes;
- (iii) Spare no effort to prevent or, if prevention is impossible, mitigate any use of its resources for ML/TF.

5. KEY PROVISIONS

The OSS shall identify, assess and understand its ML and TF risks in a way that ensures that its anti-money laundering and terrorism financing measures are commensurate with identified risks (risk-based approach) in order to make relevant decisions on how to most effectively allocate its resources. To this end, the Observatory shall apply the AML/CFTP principles through the following means:

5.1. DUE DILIGENCE

The OSS shall conduct the Counterparty Due Diligence (CDD) measures, as determined on a risk-based basis, taking into account the type of counterparty, counterparty relationship, financial instrument and country and/or region of operation. The Observatory shall identify and verify the identity of the Counterparties with which it enters in a counterparty relationship.

The OSS shall take reasonable steps to properly assess the purpose, economic rationale and general AML/CFT and related integrity aspects of counterparties and their beneficial owners in order to avoid their involvement in relation to ML and TF purposes.

The OSS shall periodically amend and improve its CDD procedures so that they will be on par with international best practices and FATF recommendations.

5.2. MONITORING

The Monitoring and Reporting Team (MRT) of the Governance Compliance and Grievance Handling Unit shall be responsible for monitoring the implementation of the Policy.

5.3. REPORTING

Any suspicious information regarding a non-legitimate or fraudulent activity (Red Flag) that comes to the knowledge of a Covered Individual indicating ML/TF, must be immediately reported by them to the MRT through any of the following means, without informing the Counterparty or other third parties (Tipping Off) that a suspicious activity is being reported or investigated:

Email:	gcghu@oss.org.tn
Hotline:	+216 71 206 633/634
Mailing Address:	Governance Compliance and Grievance Handling Unit (GCGHU). Observatoire du Sahara et du Sahel BP 31. Boulevard du Leader Yasser Arafat. Tunis 1080 Republic of Tunisia

5.4. RECORD KEEPING

The Observatory shall keep for at least 7 (seven) years all records acquired through the CDD measures and the Counterparty relationship documents and transactions carried out, as well as all correspondence with the Counterparty.

In addition to the above, the OSS shall maintain strict confidentiality in regard to information on Counterparties and transactions obtained while fulfilling AML/CFT requirements.

5.5. IMPLEMENTATION AND OBLIGATIONS

The OSS shall implement the Policy through its AML/CFT Procedures so that Covered Individuals be provided with proper guidance to smoothly and easily follow the Policy.

Also, the OSS shall not be involved with, and will terminate any existing Counterparty relationship if any, with Counterparties who:

- Do not cooperate with its CDD efforts; and/or
- Engage in activities prohibited under the OSS Prohibited Practices Policy⁷; and/or
- Are currently under any financial sanctions imposed by the United Nations.

The OSS shall terminate the existing Counterparty relationship or shall not start one if the

⁷ OSS' Prohibited Practices Policy

aforementioned Counterparty does not fully abide by the Policy.

Counterparties that do not abide by this Policy will be blacklisted by the OSS and the Observatory shall not have any kind of engagement nor relationship with the aforementioned Counterparties until they fully commit to the Policy.

Lastly, the OSS Counterparties/Partners shall be responsible for identifying and mitigating ML and TF risks, in accordance with the Policy's framework, while executing the Observatory's activities.

6. ACCOUNTABILITIES

6.1. THE EXECUTIVE SECRETARY

Has the responsibility of ensuring that the OSS governance and oversight related to ML and FT risks are properly managed through:

- The oversight of reporting and documentation of suspicious activities
- The coordination between the departments to ensure proper AML/CFT controls are in place
- The support of Department Coordinators in implementing and maintaining AML/CFT policies and procedures, therefore ensuring they are in compliance with relevant laws and regulations.

6.2. DEPARTMENT COORDINATORS

They shall assist the MRT in overseeing the reporting and documentation of suspicious activities in relation to their respective department activities. They are also responsible for communicating and disseminating AML/CFT policies and procedures inside their own unit and ensuring their respective subordinates are properly trained.

6.3. EXTERNAL AND INTERNAL AUDITS

They shall, in accordance with their own mandates, assist the MRT as may be required by the MRT in monitoring and reporting of any suspicious activities of ML/FT.

6.4. MONITORING AND REPORTING TEAM

It shall work with the Secretariat and report to the Executive Secretary, to investigate ML/FT allegations in coordination with relevant counterpart authorities.

6.5. SECRETARIAT STAFF

They shall cooperate to ensure effective implementation of the Policy, with accountabilities allocated in accordance with their respective mandates.

6.6. OTHER STAFF MEMBERS, CONSULTANTS AND OTHER ASSOCIATED PERSONS

They shall be accountable for:

- Complying with the Policy, standards and controls;

- Familiarizing themselves with and acting in accordance with relevant OSS processes and procedures to manage AML/CFT compliance; and
- Reporting to the MRT without undue delay any suspicions (or actual occurrences) or red flags of ML/TF activities.

7. EFFECTIVENESS AND REVISION

This Policy will come into effect upon its adoption by the OSS Board. It will apply to all OSS activities to the extent reasonably possible, and to those that will be approved after the effective date of this Policy.

This Policy will remain in effect until amended or superseded. It will be reviewed and updated as necessary.