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

Koson PRO Corporation
Via Espana, Delta Bank Building, 6th Floor, Suite 604D
Panama City, 0801, Republic of Panama
Company No. 155764733

1. Introduction

This Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy establishes the internal standards, principles, and procedures adopted by **Koson PRO Corporation** ("the Company") to prevent the misuse of its services for money laundering, terrorist financing, or any other illicit financial activity.

The Company operates under the laws of the Republic of Panama and acknowledges the relevance of the following frameworks:

- Law 23 of 2015 of Panama
- Executive Decree No. 363 of 2015
- Guidelines issued by competent Panamanian regulatory authorities
- Recommendations of the Financial Action Task Force (FATF)

The purpose of this Policy is to define clear internal expectations related to AML/CTF compliance, risk management, monitoring, and reporting.

2. General Responsibility for AML/CTF Compliance

The Company is responsible for ensuring AML/CTF compliance across all of its operations.

This responsibility includes:

- establishing internal standards and controls aimed at preventing financial crime

- ensuring adherence to applicable laws, regulations, and FATF-related requirements
- maintaining internal procedures for risk assessment and customer verification
- monitoring business relationships and activities on an ongoing basis
- investigating unusual or potentially suspicious behaviors
- reporting suspected illicit activity to relevant Panamanian authorities when required
- ensuring that internal staff are aware of AML/CTF obligations

Responsibility for compliance is exercised collectively at the organizational level. The Company may delegate specific tasks to employees or operational units as needed, but ultimate responsibility remains with the Company.

3. Risk-Based Approach

The Company applies a **Risk-Based Approach (RBA)** to identify, assess, and mitigate risks related to money laundering and terrorist financing.

Under this approach, the Company evaluates risks arising from:

- customer profiles and backgrounds
- ownership structures
- geographic exposure
- the nature of services requested
- transaction patterns and expected behavior
- any use of digital or virtual assets, where applicable

Higher-risk factors may require enhanced internal scrutiny and additional information.

4. Customer Due Diligence (CDD)

The Company maintains internal procedures for Customer Due Diligence proportionate to its risk exposure. These procedures may include:

- identifying customers and collecting basic information
- verifying identity through appropriate documentation or data sources
- identifying beneficial owners of legal entities
- understanding the intended nature of the business relationship
- assessing the legitimacy of the customer's source of funds where relevant

CDD measures are applied at the start of a business relationship and periodically updated whenever necessary based on risk.

5. Enhanced Due Diligence (EDD)

Where higher risks are identified, the Company may apply Enhanced Due Diligence measures, which may include:

- obtaining additional customer information
- conducting deeper verification of identities and ownership
- assessing customer activities with greater scrutiny
- reviewing the purpose of complex or unusual transactions
- obtaining further evidence of the source of funds or wealth

Situations that may trigger EDD include, but are not limited to:

- customers from high-risk jurisdictions
- complex corporate structures
- activities that deviate from expected patterns

- circumstances with elevated exposure to financial crime risks

6. Ongoing Monitoring

The Company monitors its business relationships and customer activity on a continuous basis to ensure consistency with expected behavior.

Monitoring practices may include:

- reviewing transactions for reasonableness
- identifying unusual patterns or deviations
- evaluating the context of financial movements
- applying additional checks when activity appears inconsistent
- documenting any findings that may require further review

Unusual activity is subject to internal assessment and, if necessary, escalation.

7. Suspicious Activity Review and Reporting

If the Company identifies activity that appears unusual, inconsistent with customer information, or potentially related to money laundering or terrorist financing, the Company will:

1. review the activity internally
2. collect relevant information and assess whether it may constitute suspicion
3. determine whether a report to Panamanian authorities is required

Where legally required, reports may be submitted to the appropriate competent authority in Panama.
No employee or representative may disclose to any customer or third party that a review or report is in progress.

8. Record Keeping

The Company maintains internal records relevant to AML/CTF compliance, including:

- customer identification and verification data
- documentation related to beneficial ownership
- records of due diligence and risk assessments
- transaction information
- internal reviews or findings related to unusual activity
- supporting documentation for any regulatory filings

Records are retained for the minimum period required under Panamanian law or longer if deemed necessary by the Company.

9. Sanctions Compliance

The Company does not knowingly engage with persons, entities, or jurisdictions subject to sanctions issued by:

- the United Nations
- the United States (OFAC)
- the European Union
- the United Kingdom
- relevant Panamanian authorities

Screening may be carried out at onboarding and periodically thereafter.

10. Use of Digital or Virtual Assets (if applicable)

If the Company interacts with digital or virtual assets, it will implement internal precautions including:

- verifying ownership of external wallets where relevant
- reviewing transfers that appear unusual or inconsistent
- conducting additional checks where external data or wallet information is incomplete
- ensuring compliance with FATF guidance related to digital assets

Unverifiable or unexplained activity may trigger internal review.

11. Staff Awareness

The Company maintains internal awareness of AML/CTF obligations through:

- internal instructions and guidelines
- periodic informational updates
- availability of compliance-related documentation to relevant personnel

Staff are expected to follow internal procedures and report any unusual behavior to the Company's designated internal review structure.

12. Policy Review and Updates

The Company periodically reviews and updates this Policy to ensure continued alignment with:

- changes in applicable laws or regulations
- evolving FATF recommendations
- internal risk assessments
- updates in business activities or operational models

Any modifications are adopted at the Company’s discretion.

13. Contact Information

For questions, requests, or concerns regarding this AML Policy, please contact us at:

Koson PRO Corporation
Via Espana, Delta Bank Building, 6th Floor, Suite 604D
Panama City, 0801, Republic of Panama
Email: info@kosonpro.com