ANTI-MONEY LAUNDERING & COUNTER-TERRORISM FINANCING POLICY

Kairos 777 Inc. -- Version 1.0

Kairos 777 Inc.

February 27, 2026

Field	Value
Document	AML/CTF Compliance Policy
Version	1.0
Effective Date	February 27, 2026
Last Reviewed	February 27, 2026
Approved By	Mario Isaac, Founder & Director
Entity	Kairos 777 Inc.

1. Purpose & Scope

1.1 Purpose

This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy establishes the framework by which Kairos 777 Inc. ("the Company") identifies, assesses, mitigates, and reports risks related to money laundering (ML), terrorism financing (TF), and other financial crimes in connection with the operation of the Kairos ecosystem, including:

* Kairos Coin (KAIROS) -- USD-pegged stablecoin
* Kairos Trade -- Automated trading platform
* Kairos Wallet -- Multi-chain digital wallet

1.2 Scope

This policy applies to:

* All officers, directors, employees, and contractors of Kairos 777 Inc.
* All blockchain transactions involving KAIROS tokens across all deployed chains (BSC, Base, Arbitrum, Polygon)
* All fiat-to-crypto on-ramp transactions facilitated through third-party partners (e.g., Transak)
* All redemption processes (KAIROS to stablecoin conversions)
* All minting and burning operations

1.3 Regulatory Framework

This policy is designed with reference to:

* U.S. Bank Secrecy Act (BSA) and its implementing regulations
* FinCEN guidance on virtual currency (FIN-2019-G001)
* OFAC sanctions compliance requirements
* FATF Recommendations on virtual assets and VASPs
* EU Anti-Money Laundering Directives (5AMLD/6AMLD)

2. Risk Assessment

2.1 ML/TF Risk Factors

Risk Category	Level	Mitigation

Product: Stablecoin	Medium	On-chain transparency, blacklisting
Geography: Global	High	KYC via licensed partners, OFAC screening
Transaction: Large value	Medium	Threshold monitoring ($10K+)
Customer: Anonymous wallets	Medium	KYC delegation to Transak
Channel: Decentralized	Medium	On-chain monitoring, events
Minting: Centralized	Low	Single authorized owner, audit trail

2.2 Inherent Risk Mitigations

* Public blockchain transparency: All transactions are permanently recorded and auditable.
* Stablecoin nature: Fixed 1:1 USD peg removes speculative value fluctuation.
* On-chain compliance tools: Blacklisting, pause mechanism, and event logging built into smart contract.
* KYC-gated fiat on-ramp: All fiat-to-KAIROS purchases go through licensed KYC providers.

3. Customer Due Diligence (CDD)

3.1 Fiat On-Ramp Purchases (via Transak)

* KYC is performed by Transak in accordance with their licensed compliance program
* Transak verifies customer identity, performs sanctions screening, and maintains KYC records
* Kairos 777 Inc. receives confirmation of successful KYC verification before token transfer
* Records of all Transak-facilitated transactions are maintained by both parties

3.2 Direct Crypto Purchases (On-Chain)

* Transactions occur on public blockchains without direct intermediation by Kairos 777 Inc.
* The Company monitors on-chain activity for suspicious patterns through blockchain analytics
* The blacklisting mechanism allows freezing addresses associated with illicit activity

3.3 Enhanced Due Diligence (EDD)

Enhanced due diligence is applied for:

* Transactions exceeding $10,000 USD equivalent in a single transaction
* Cumulative activity exceeding $50,000 USD within a 30-day period from a single address
* Addresses flagged by blockchain analytics as associated with sanctioned entities, mixing services, darknet markets, or ransomware
* Transactions involving FATF high-risk jurisdictions

4. Transaction Monitoring

4.1 On-Chain Monitoring

Monitor	Method	Frequency

Minting events	Smart contract event listener	Real-time
Burning events	Smart contract event listener	Real-time
Large transfers	Backend API monitoring	Real-time
Fee collection	FeeCollected event tracking	Real-time
Blacklist actions	Event tracking	Real-time
Total supply changes	totalMinted/totalBurned	Daily reconciliation

4.2 Alert Thresholds

Trigger	Threshold	Action
Single transaction	> $10,000 USD	Automated alert + manual review
Cumulative (30-day)	> $50,000 USD	Enhanced review + EDD
Rapid transactions	> 10 in 1 hour	Pattern analysis review
Flagged address	Any amount	Immediate review + blacklisting
Minting event	Any amount	Logged + Director notification
Redemption	> $10,000 USD	Manual verification required

4.3 Monitoring Tools

* Backend API: Real-time monitoring across all 4 deployed chains
* BscScan/Block Explorer Alerts: Configured for key wallet addresses
* Transaction Log Database: Turso database with 5-year retention
* Manual Review: Periodic review of large transactions and unusual patterns

5. Sanctions Screening

5.1 OFAC Compliance

The Company screens against:

* OFAC SDN (Specially Designated Nationals) List
* OFAC Consolidated Sanctions List
* EU Consolidated List of Sanctions
* UN Security Council Sanctions List

5.2 Screening Process

* All addresses interacting with minting, burning, or redemption functions are screened
* Blockchain analytics identify indirect connections to sanctioned entities
* Sanctioned addresses are immediately blacklisted via smart contract
* Blacklisting is permanent until explicitly removed by the contract owner

5.3 High-Risk Jurisdictions

The Company does not knowingly facilitate services to users in:

* North Korea (DPRK)
* Iran
* Syria
* Cuba
* Crimea, Donetsk, and Luhansk regions
* Any other jurisdiction subject to comprehensive OFAC sanctions

6. Suspicious Activity Reporting

6.1 SAR Filing

When suspicious activity is identified, the Company will:

* Document the suspicious activity with all relevant transaction details
* Review internally within 24 hours of detection
* File a SAR with FinCEN within 30 calendar days (or 60 days if no suspect identified)
* Retain all supporting documentation for a minimum of 5 years
* Blacklist the associated address(es) on-chain if appropriate

6.2 Red Flags

* Structuring: Multiple transactions just below reporting thresholds
* Rapid movement: Tokens received and immediately transferred to different addresses
* Mixing patterns: Tokens routed through multiple wallets in quick succession
* Geographic risk: Activity from or to high-risk jurisdictions
* Unusual redemptions: Large redemptions without corresponding legitimate activity
* Address clustering: Multiple wallets controlled by same entity suggesting obfuscation

7. Record Keeping

7.1 Retention Requirements

Record Type	Retention	Storage
On-chain transaction logs	Permanent	Blockchain (immutable)
Backend transaction logs	5 years min	Turso cloud database
Minting/burning records	5 years min	Turso + blockchain
KYC records	Per Transak policy	Maintained by Transak
SAR filings	5 years from filing	Secure encrypted storage
Compliance review records	5 years	Secure encrypted storage
Blacklist action records	Permanent	Blockchain events + DB

7.2 Data Security

* Encryption at rest and in transit (TLS/HTTPS)
* Access restricted to authorized compliance personnel
* Regular backup procedures
* Secure cloud infrastructure (Render, Turso)

8. On-Chain Compliance Mechanisms

8.1 Address Blacklisting

```
Function: blacklist(address account)
Effect: Permanently prevents sending or receiving KAIROS
Event: Blacklisted(address indexed account)
Authority: Contract owner only
```

8.2 Emergency Pause

```
Function: pause()
Effect: Halts ALL token transfers, minting, and burning
Event: Paused(address account)
Authority: Contract owner only
Use Case: Discovered exploit, regulatory order, or emergency
```

8.3 Audit Trail

Action	Event Emitted
Token minting	Mint(address indexed to, uint256 amount)
Token burning	Burn(address indexed from, uint256 amount)
Address blacklisted	Blacklisted(address indexed account)
Address unblacklisted	UnBlacklisted(address indexed account)
Fee rate changed	FeeUpdated(uint256 old, uint256 new)
Contract paused	Paused(address account)
Contract unpaused	Unpaused(address account)

9. Compliance Officer

Field	Value
Name	Mario Isaac
Title	Founder, Director & Compliance Officer
Entity	Kairos 777 Inc.
Email	info@kairos-777.com

The Compliance Officer is responsible for:

* Overall implementation and enforcement of this AML/CTF policy
* Reviewing and approving all blacklist actions
* Filing SARs when required
* Conducting periodic risk assessments (at minimum quarterly)
* Ensuring all monitoring systems are operational
* Staying current with regulatory developments

10. Training & Awareness

* Initial training upon assuming role: AML/CTF policy, red flags, reporting, sanctions
* Annual refresher training on updated regulations and emerging risks
* Ad-hoc training when significant regulatory changes occur

11. Policy Review & Updates

This policy is reviewed and updated:

* Annually at minimum
* Upon significant regulatory changes affecting virtual assets or stablecoins
* Upon material changes to the Company operations or product offerings
* After any compliance incident requiring policy adjustment

12. Version History

Version	Date	Author	Changes
1.0	February 27, 2026	Mario Isaac	Initial policy creation

Approved by:

Mario Isaac

Founder, Director & Compliance Officer

Kairos 777 Inc.

February 27, 2026

"In God We Trust"