KwanzaPay Anti-Money Laundering (AML) Policy

Effective Date: November 7, 2024

1. Introduction

This Anti-Money Laundering (AML) Policy establishes KwanzaPay's comprehensive framework for preventing, detecting, and reporting money laundering, terrorist financing, and other financial crimes through our platform. The policy applies to all KwanzaPay employees, contractors, platform users, merchants, third-party service providers, and affiliated entities across all supported jurisdictions.

KwanzaPay maintains strict compliance with the Nigerian Money Laundering (Prevention and Prohibition) Act, FATF Recommendations, and applicable local regulatory requirements. Our commitment extends to following international standards, industry best practices, and specific cryptocurrency guidelines while adhering to digital asset regulations and counter-terrorist financing requirements.

2. Risk-Based Approach

Risk Assessment Framework

Our risk assessment framework evaluates multiple factors to ensure comprehensive risk management. Customer risk factors include geographic location, transaction patterns, account types, and business nature, with particular attention to source of funds and trading volumes. Product risk assessment encompasses cryptocurrency types, transaction limits, and various platform features including P2P trading and fiat gateways.

Geographic risk factors receive careful consideration, including regulatory status, local compliance requirements, and international cooperation capabilities. We maintain heightened scrutiny for high-risk jurisdictions and sanctioned countries, incorporating appropriate risk mitigation measures based on regional risk profiles.

Risk Mitigation

KwanzaPay implements robust control measures including sophisticated transaction monitoring, comprehensive screening systems, and stringent verification procedures. Our risk mitigation framework incorporates automated alert systems and thorough documentation requirements, ensuring proper audit trails and compliance verification.

Enhanced Due Diligence (EDD) procedures apply to high-risk customers, large transactions, and complex structures. These procedures include detailed source of wealth verification and extensive documentation requirements for high-risk jurisdictions or politically exposed persons.

3. Customer Due Diligence (CDD)

Basic Due Diligence

Our standard due diligence process requires comprehensive identity verification through government-issued identification, proof of address, and multi-factor authentication methods. This process includes thorough validation of user information including full legal name, date of birth, residential address, and contact details. We verify tax residency and employment status while assessing the intended purpose of account usage and expected activity patterns.

Enhanced Due Diligence

Enhanced Due Diligence triggers include high transaction volumes, high-risk jurisdictional exposure, and complex transaction patterns. Additional requirements may include detailed bank statements, comprehensive source of wealth documentation, and business registration verification for corporate accounts. We maintain stringent protocols for political exposure assessment and cross-border activity monitoring.

4. Transaction Monitoring

Monitoring Framework

KwanzaPay employs sophisticated automated monitoring systems incorporating real-time transaction screening, advanced pattern detection algorithms, and behavioral analytics. Our monitoring framework includes comprehensive wallet clustering analysis and blockchain analytics integration, ensuring thorough oversight of all platform activity.

The system monitors cryptocurrency deposits and withdrawals, fiat currency transactions, P2P trading patterns, and cross-border movements. Special attention focuses on payment method usage patterns, trading frequency analysis, and device usage monitoring to identify potential risks.

Risk Indicators

Our transaction monitoring system identifies specific red flags including structured transactions, suspicious rapid movements, and unusual trading hours. Special attention focuses on high-risk wallet interactions and privacy coin conversion attempts. Trading red flags encompass potential price manipulation, wash trading patterns, and suspicious cancellation behavior.

Investigation Procedures

KwanzaPay maintains comprehensive investigation protocols for all identified alerts. Each investigation encompasses thorough data collection, pattern analysis, and customer profile review. Our investigation team conducts detailed transaction history analysis while maintaining comprehensive documentation of findings and decisions. Regular review ensures investigation quality and consistency across all cases.

5. Reporting Requirements

Suspicious Activity Reports (SARs)

KwanzaPay maintains stringent procedures for identifying and reporting suspicious activity. Filing triggers include unusual transaction patterns, multiple red flag indicators, and compliance concerns. Our reporting process ensures thorough documentation and timely submission to relevant authorities while maintaining appropriate confidentiality measures.

The SAR filing process includes comprehensive information gathering, detailed report preparation, and thorough quality review before submission. Our system maintains robust record-keeping procedures and implements appropriate follow-up measures for all reported cases.

Regulatory Reporting

Beyond SARs, KwanzaPay fulfills all regulatory reporting obligations including large transaction reports, currency transaction reports, and cross-border transaction reporting requirements. We maintain strict adherence to reporting timeframes, ensuring immediate reporting for urgent matters and systematic submission of periodic compliance reports.

6. Training and Compliance

Employee Training

KwanzaPay implements comprehensive training programs encompassing new hire orientation, regular refresher courses, and specialized role-specific training. Our curriculum covers AML regulations, KYC procedures, and emerging industry developments. Training materials incorporate practical case studies and real-world scenarios to enhance understanding and application.

Compliance Monitoring

Internal compliance monitoring ensures adherence to established policies and procedures through regular audits and systematic quality assurance reviews. Our monitoring program evaluates policy compliance, procedure adherence, and overall system effectiveness while maintaining detailed performance metrics and improvement tracking.

7. Sanctions Compliance

Screening Requirements

Our sanctions compliance program implements comprehensive screening across customer onboarding, ongoing monitoring, and transaction processing. The screening scope includes wallet addresses, payment methods, business partners, and connected entities. We maintain thorough screening against major sanctions lists including OFAC SDN List, UN Sanctions Lists, and relevant local watchlists.

Match Handling

Identified sanctions matches undergo immediate review following established escalation procedures. Our process includes thorough false positive analysis and comprehensive documentation requirements. When necessary, we implement immediate account restrictions and asset freezing measures while maintaining appropriate communication protocols with relevant authorities.

8. Record Keeping

Documentation Requirements

KwanzaPay maintains comprehensive records of all customer information, transaction details, and compliance activities. Customer records include identification documents, verification results, and due diligence findings. Transaction records encompass complete details of all platform activity including blockchain data and supporting documentation.

Retention Requirements

Our record retention policy adheres to regulatory requirements with specific retention periods for different document categories. Customer data and transaction records are maintained for seven years, while investigation files and regulatory reports are retained for five years. All records are stored in secure systems with appropriate access controls and encryption standards.

9. Emergency Procedures

Immediate Actions

KwanzaPay maintains clear protocols for immediate response to suspicious activities, including account freezing, transaction blocking, and evidence preservation measures. Our emergency procedures ensure prompt authority notification while maintaining appropriate customer communication channels.

Business Continuity

Our business continuity planning encompasses comprehensive contingency measures for system failures, data breaches, and external emergencies. We maintain detailed communication plans for internal notification, external communications, and regulatory reporting during emergency situations.

10. Policy Management

Policy Maintenance

This policy undergoes regular review and updates to maintain alignment with regulatory requirements and industry best practices. Updates incorporate emerging risks, regulatory changes, and operational improvements while ensuring continued effectiveness of our AML program.

Compliance Oversight

The Compliance Officer maintains primary responsibility for policy oversight and program management. Our governance structure ensures appropriate board oversight, committee reviews, and management reporting while maintaining clear escalation procedures and decision authority.

This policy is effective immediately and supersedes all previous versions.

Last Updated: November 7, 2024

Approved by: Chief Compliance Officer Board of Directors

KwanzaPay Limited