This Anti-Money Laundering and Compliance Policy ("AML Policy") sets out the framework by which Kuro Network Global LLC ("Kuro Network", "we", "us") identifies, assesses, and mitigates the risk of money laundering, terrorist financing, fraud, and other financial crimes in connection with the services we provide. All staff, contractors, and officers of Kuro Network are required to comply with this policy.

Effective Date: Upon adoption · Registered Jurisdiction: United States · Governing Framework: US Bank Secrecy Act (BSA), OFAC Sanctions, FinCEN Guidelines

**TABLE OF CONTENTS**



## 01 PURPOSE & SCOPE

WHAT THIS POLICY COVERS AND WHO IT APPLIES TO

Kuro Network provides managed Meta advertising infrastructure to businesses and media buyers worldwide. Our services involve the receipt and processing of payments via bank transfer and cryptocurrency, which creates an obligation to maintain appropriate safeguards against financial crime.

| | |
|---|---|
| **PURPOSE** | To establish clear procedures for detecting, preventing, and reporting money laundering, terrorist financing, fraud, and related financial crimes across all Kuro Network operations and client relationships. |

| | |
|---|---|
| **SCOPE** | This policy applies to all Kuro Network employees, contractors, directors, and any individual acting on behalf of the company. It covers all client onboarding, payment processing, and account management activities. |
| **LEGAL BASIS** | Kuro Network Global LLC is incorporated in the United States. Although operations are conducted internationally, US incorporation means the company remains subject to the US Bank Secrecy Act (BSA), Office of Foreign Assets Control (OFAC) sanctions requirements, and FinCEN guidance — which apply to all US-registered entities regardless of where business is conducted. |
| **ZERO TOLERANCE** | Kuro Network maintains a zero-tolerance policy toward money laundering, terrorist financing, and financial fraud. Any client or internal party found to be engaged in such activity will be reported to the relevant authorities and all services will be terminated immediately without refund. |

## 02 DESIGNATED AML COMPLIANCE OFFICER

ROLE, RESPONSIBILITIES & APPOINTMENT

**AML OFFICER — ROLE TO BE FORMALLY APPOINTED**

- Kuro Network is in the process of formally designating a named AML Compliance Officer ("AMLCO"). Until a dedicated officer is appointed, AML compliance responsibilities are managed at the founder / director level.
- The AMLCO will serve as the primary point of contact for all AML-related matters, internal escalations, and regulatory reporting obligations.
- The appointment of a formal AMLCO is a priority action item under this policy and must be completed within 90 days of adoption.

| | |
|---|---|
| **RESPONSIBILITIES** | The AMLCO is responsible for: maintaining and updating this AML Policy; overseeing client due diligence procedures; reviewing flagged transactions; filing Suspicious Activity Reports (SARs) with FinCEN where required; and ensuring all team members receive adequate AML training. |
| **AUTHORITY** | The AMLCO has the authority to pause, restrict, or terminate any client account pending investigation without prior approval from other directors, where there is reasonable suspicion of financial crime. |
| **ESCALATION** | Any team member who suspects money laundering or financial crime must escalate immediately to the AMLCO (or acting director). Internal escalation must occur within 24 hours of suspicion arising. |

| | |
|---|---|
| **INDEPENDENCE** | The AMLCO must operate independently of commercial pressures and must not be placed in a position where business development objectives could compromise the integrity of compliance decisions. |

## 03 CUSTOMER DUE DILIGENCE (KYC)

KNOW YOUR CUSTOMER — ONBOARDING & VERIFICATION

Customer Due Diligence (CDD) is the process by which Kuro Network identifies and verifies the identity of clients before providing services. Our current baseline CDD standard and future enhancement roadmap are outlined below.

**CURRENT KYC STANDARD — BASELINE LEVEL**

- At present, Kuro Network collects email address and business/company name as the minimum standard for client identification at onboarding.
- Government-issued ID is not required as standard. Clients are not asked to provide formal identification documents unless suspicious activity or circumstances warranting further scrutiny arise.
- Where concerns are identified, additional verification steps may be requested at the AMLCO's discretion.

| | |
|---|---|
| **STANDARD CDD** | All new clients must provide: a valid email address; their registered company or business name; a billing address; and a phone number. This information is verified for consistency at the point of onboarding. |
| **ENHANCED SCRUTINY** | Where a client's activity, payment patterns, or profile raise concerns — including unusually high transaction volumes, inconsistent information, or OFAC/PEP flags — the AMLCO may request additional information. This may include source of funds documentation or, where genuinely warranted by suspicion, formal identity verification. Such requests are made on a case-by-case basis and are not a standard onboarding requirement. |
| **ONGOING MONITORING** | Client profiles are subject to ongoing review. Where a client's activity changes materially — such as a significant increase in spend volume or changes to payment methods — refreshed due diligence may be required. |
| **RIGHT TO REFUSE** | Kuro Network reserves the right to refuse onboarding or to terminate an existing client relationship where satisfactory due diligence cannot be completed, without being required to provide a reason. |

# 04 CRYPTOCURRENCY & PAYMENT SCREENING

CRYPTO TOP-UP CONTROLS & SOURCE OF FUNDS

Kuro Network accepts cryptocurrency as a payment method for top-ups. Cryptocurrency transactions carry a heightened risk of anonymity and potential misuse for money laundering. The following controls apply to all crypto payments received:

**CRYPTO RISK ACKNOWLEDGEMENT**

- Kuro Network acknowledges that cryptocurrency payments are currently accepted without automated blockchain screening or wallet address verification.
- This is identified as a compliance risk area. Implementation of a crypto screening solution (e.g. Chainalysis, Elliptic, or equivalent) is a priority action item under this policy.
- Until automated screening is in place, the manual controls below apply to all cryptocurrency transactions.

| | |
|---|---|
| **ACCEPTED CURRENCIES** | Only widely-used, publicly traceable cryptocurrencies are accepted. Kuro Network does not accept privacy coins (e.g. Monero, Zcash) under any circumstances. |
| **TRANSACTION LIMITS** | Crypto top-ups above $5,000 in a single transaction will trigger a manual review by the AMLCO prior to funds being credited to the client account. The client may be asked to provide source of funds documentation. |
| **WALLET CONSISTENCY** | Clients must transact from the same wallet address on record. Payments received from unregistered or inconsistent wallet addresses will be flagged for review and may be held pending verification. |
| **REFUND ROUTING** | In line with our Terms of Service, crypto refunds in the event of service failure are issued to a verified bank account — not returned to a crypto address — to maintain a clear audit trail. |
| **PROHIBITED SOURCES** | Kuro Network will not knowingly accept cryptocurrency originating from darknet markets, mixing services, sanctioned addresses, or any source flagged by OFAC. Such transactions will be reported to FinCEN via SAR. |
| **FUTURE SCREENING** | Kuro Network commits to implementing an automated crypto transaction screening tool within 6 months of this policy's adoption date, to bring crypto due diligence in line with best practice. |

# 05 SANCTIONS COMPLIANCE — OFAC

US OFFICE OF FOREIGN ASSETS CONTROL

As a US-incorporated entity, Kuro Network is legally required to comply with all sanctions programmes administered by the US Office of Foreign Assets Control (OFAC). This obligation applies to all US-registered entities regardless of where operations are physically conducted. The following controls are in place:

| | |
|---|---|
| **PROHIBITED PERSONS** | Kuro Network will not provide services to any individual, entity, or organisation listed on the OFAC Specially Designated Nationals (SDN) list or any other US sanctions list. All prospective clients are subject to screening against current OFAC lists at onboarding. |
| **PROHIBITED COUNTRIES** | Services are not available to clients located in, or acting on behalf of individuals or entities in, comprehensively sanctioned countries or regions including but not limited to: Cuba, Iran, North Korea, Russia (select sectors), Syria, and the Crimea/Donetsk/Luhansk regions of Ukraine. |
| **ONGOING SCREENING** | Existing client accounts are subject to periodic re-screening against updated OFAC sanctions lists. Where a match is identified on an existing account, services will be suspended immediately and the matter escalated to the AMLCO. |
| **FALSE POSITIVES** | Where a sanctions screening match is identified that appears to be a false positive, the AMLCO will conduct a reasonable review before services are resumed. The client may be asked to provide identity documentation to resolve the match. |
| **REPORTING OBLIGATION** | Where a confirmed sanctions match is identified, Kuro Network is legally obligated to block the transaction, freeze associated funds, and report the matter to OFAC within 10 days via the required reporting process. No notification will be given to the client. |

## 06 POLITICALLY EXPOSED PERSONS (PEPs)

DEFINITION, IDENTIFICATION & ENHANCED CHECKS

### WHAT IS A POLITICALLY EXPOSED PERSON (PEP)?

- A Politically Exposed Person (PEP) is any individual who holds or has held a prominent public function — including heads of state, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned enterprises, or senior officials of political parties.
- The definition also extends to immediate family members (spouses, children, parents, siblings) and known close associates of such individuals.
- PEPs are not prohibited from using Kuro Network services, but they are subject to Enhanced Due Diligence (EDD) due to the elevated risk of corruption and bribery associated with their positions.

| | |
|---|---|
| **IDENTIFICATION** | All new clients are subject to PEP screening at onboarding. Where a client self-identifies or is identified as a PEP, the case is escalated to the AMLCO before services are activated. |

| | |
|---|---|
| **ENHANCED SCRUTINY** | PEP clients are subject to closer monitoring and senior management awareness before services are activated. Additional information — such as source of funds context or business purpose — may be requested at the AMLCO's discretion. Formal government-issued ID is only requested where specific circumstances or suspicious indicators make it warranted, not as an automatic requirement. |
| **ONGOING MONITORING** | Existing clients who become PEPs during their subscription (e.g. through election or appointment) must notify Kuro Network promptly. Failure to disclose PEP status is grounds for immediate account termination. |
| **HIGHER-RISK PEPs** | PEPs from higher-risk jurisdictions — particularly those with elevated corruption indices as assessed by Transparency International — are subject to additional scrutiny and may be declined at the AMLCO's discretion. |

## 07 TRANSACTION MONITORING

FLAGGING UNUSUAL & SUSPICIOUS ACTIVITY

Kuro Network monitors all client transactions for unusual patterns or activity that may indicate financial crime. The following framework governs how transactions are reviewed and escalated:

| | |
|---|---|
| **MANUAL MONITORING** | All client top-ups and payment activity are reviewed manually by the compliance team. Unusual patterns — including sudden spikes in top-up volume, irregular payment timing, or inconsistent wallet addresses — are flagged for AMLCO review. |
| **THRESHOLD — CRYPTO** | Individual cryptocurrency transactions of $5,000 or more trigger an automatic manual review before funds are credited. The client may be requested to provide source of funds documentation. |
| **THRESHOLD — BANK** | Bank transfers of $10,000 or more in a single transaction, or a cumulative $10,000 within a rolling 30-day period from a single client, trigger a mandatory review under BSA Currency Transaction Reporting obligations. |
| **RED FLAGS** | The following patterns are treated as automatic red flags: multiple small payments structured to avoid thresholds (structuring); payments from multiple unrelated sources for one account; clients unwilling to provide source of funds when requested; payments received from or refunds requested to third-party accounts; sudden large top-ups inconsistent with the client's stated business profile. |
| **STRUCTURING** | Deliberately breaking up payments to avoid reporting thresholds ("structuring") is a federal offence under the BSA. Any suspected structuring will result in immediate account suspension and SAR filing. |
| **ESCALATION TIMELINE** | Flagged transactions must be reviewed by the AMLCO within 48 hours of being raised. If the review cannot be completed within this window, the relevant top-up will remain on hold until cleared. |

## 08 SUSPICIOUS ACTIVITY REPORTING (SAR)

INTERNAL ESCALATION & REGULATORY FILING

Where Kuro Network suspects or has reasonable grounds to believe that a client is engaged in money laundering, terrorist financing, or related financial crime, we are obligated to file a Suspicious Activity Report (SAR) with FinCEN. The process is as follows:

| | |
|---|---|
| **INTERNAL ESCALATION** | Any team member who identifies suspicious activity must report it to the AMLCO immediately and no later than 24 hours after the suspicion arises. Reports must be made in writing, detailing the nature of the concern, the client involved, and the relevant transaction(s). |
| **AMLCO REVIEW** | The AMLCO will review all internal escalations within 48 hours. If the AMLCO determines that a SAR is required, it must be filed with FinCEN within 30 days of the date on which suspicion arose, or within 30 days of detection where no suspect was initially identified. |
| **SAR FILING** | SARs are filed electronically via the FinCEN BSA E-Filing System. Each SAR must include: a description of the suspicious activity; the identities of parties involved where known; relevant transaction details; and the basis for suspicion. |
| **TIPPING OFF — PROHIBITED** | It is a criminal offence to inform a client or any third party that a SAR has been or may be filed against them ("tipping off"). Any team member who becomes aware of a SAR filing must maintain strict confidentiality. Violation of this rule will result in immediate dismissal and may constitute a criminal offence. |
| **ACCOUNT ACTION** | Pending the outcome of a SAR review, the client's account may be suspended, top-ups withheld, and services restricted at the AMLCO's discretion. No explanation will be provided to the client during this period. |
| **NO RETALIATION** | No team member will face any adverse action for making a genuine, good-faith internal report of suspected financial crime, even if the suspicion proves to be unfounded following investigation. |

## 09 RECORD KEEPING

TRANSACTION LOGS & COMPLIANCE RECORDS

Kuro Network maintains comprehensive records of all client transactions and onboarding information. Accurate record-keeping is essential both for internal compliance review and for meeting regulatory obligations under the BSA.

| | |
|---|---|
| **WHAT WE RECORD** | All client onboarding data (email, business name, billing address, phone); all top-up transactions including amount, date, payment method, and reference; all refund transactions; all internal compliance flags and AMLCO review outcomes; and all SAR filings. |

| | |
|---|---|
| **RETENTION PERIOD** | All AML-related records — including transaction logs, due diligence documentation, and SAR filings — are retained for a minimum of five (5) years from the date of the transaction or the date the client relationship ended, whichever is later. This meets the BSA minimum retention requirement. |
| **STORAGE & SECURITY** | Records are stored on secure, access-controlled servers. Access to AML records is restricted to the AMLCO, senior management, and authorised compliance personnel only. |
| **REGULATORY ACCESS** | Records will be made available to regulatory authorities — including FinCEN, OFAC, or law enforcement — upon receipt of a valid legal request or court order. Kuro Network will cooperate fully with all lawful investigations. |

## 10 STAFF TRAINING

AML AWARENESS & ONGOING EDUCATION

**CURRENT TRAINING STATUS**

- AML training is currently conducted at the founder / compliance lead level. This policy establishes the framework for expanding training requirements across the full team as Kuro Network grows.
- All new hires who interact with client accounts or payments must complete AML awareness training before commencing their role.

| | |
|---|---|
| **MANDATORY TRAINING** | All personnel with access to client accounts, payment data, or compliance systems must complete AML awareness training. This includes understanding of: what money laundering is and how it occurs; red flags and suspicious activity indicators; internal reporting obligations; and the consequences of non-compliance. |
| **FREQUENCY** | Initial training must be completed before a team member begins work. Refresher training is required annually, or sooner where there are material changes to this policy or applicable regulations. |
| **AMLCO TRAINING** | The designated AMLCO must maintain up-to-date knowledge of AML regulations, FinCEN guidance, and OFAC requirements. External training, certification, or professional development is strongly encouraged and should be undertaken at least annually. |
| **TRAINING RECORDS** | Records of all training completed — including dates, content covered, and personnel trained — must be maintained by the AMLCO and retained for a minimum of five (5) years. |

## 11 POLICY REVIEW & UPDATES

KEEPING THIS POLICY CURRENT

This AML Policy is a living document. It will be reviewed and updated regularly to reflect changes in regulation, business operations, and risk environment.

| | |
|---|---|
| **ANNUAL REVIEW** | This policy must be formally reviewed by the AMLCO and senior management at least once every twelve (12) months, or sooner if triggered by a regulatory change, a significant incident, or a material change to Kuro Network's business model. |
| **TRIGGERED REVIEW** | An unscheduled review is required following: any confirmed SAR filing; a regulatory enquiry or audit; the introduction of new payment methods; significant client base growth; or entry into higher-risk market verticals. |
| **VERSION CONTROL** | Each version of this policy must be dated, numbered, and archived. Superseded versions are retained for a minimum of five (5) years for audit purposes. |
| **STAFF NOTIFICATION** | All team members must be notified of material policy updates and must acknowledge receipt and understanding of the revised policy within 14 days of the update being issued. |

## 12 CONTACT & OFFICER DETAILS

AML ESCALATION & COMPLIANCE CONTACTS

For all AML-related enquiries, internal escalations, or compliance concerns, contact the designated compliance lead using the details below.

| | |
|---|---|
| **COMPANY** | Kuro Network Global LLC |
| **REGISTERED JURISDICTION** | United States (incorporated) — operations conducted internationally |
| **GOVERNING FRAMEWORK** | US Bank Secrecy Act · OFAC · FinCEN Guidelines |
| **COMPLIANCE LEAD** | luca@kuronet.io |
| **GENERAL SUPPORT** | contact@kuronet.io |
| **SUPPORT CHANNELS** | WhatsApp · Telegram · Discord |

| AML OFFICER STATUS | Pending formal appointment — currently managed at director level |
|---|---|

## POLICY ADOPTION & COMMITMENT

This AML & Compliance Policy has been adopted by Kuro Network Global LLC and is binding on all personnel, contractors, and representatives of the company. Failure to comply with this policy may result in disciplinary action, termination of engagement, and potential referral to law enforcement authorities. This policy is to be read alongside the Kuro Network Terms of Service and Privacy Policy.

For all compliance escalations or AML concerns, contact the compliance lead directly at luca@kuronet.io.