FORMATNULL VENTURES

Anti-Money Laundering (AML)

Due Diligence Procedures & Exchange Partner Compliance Framework

Document Classification	Confidential - Compliance
Prepared by	Joshua Hall
Effective Date	May 1, 2026
Version	1.0
Next Review Date	November 1, 2026
Approved by	Joshua Hall, Managing Partner & Compliance Officer
Regulatory Framework	FATF Recommendations; Hong Kong AMLO; VASP Guidelines

Restricted distribution. Prepared for institutional due diligence and exchange partner review.

Table of Contents

Right-click and update field to refresh the table of contents.

Note: In Microsoft Word, right-click the table above and select "Update Field" to refresh page numbers after editing.

1. Purpose & Scope

1.1 Purpose

This document establishes the Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and due diligence procedures for Formatnull Ventures ("the Firm") in its capacity as a systematic trading firm operating across centralized cryptocurrency exchanges. These procedures are designed to:

1. **Prevent** the Firm's trading infrastructure and capital from being exploited for money laundering, terrorist financing, sanctions evasion, or other financial crimes
2. **Comply** with applicable anti-money laundering laws, regulations, and international standards
3. **Assess and manage** the ML/TF risks arising from the Firm's relationships with exchange partners
4. **Demonstrate** to exchange partners and counterparties that the Firm maintains institutional-grade compliance standards
5. **Protect** the Firm's reputation and operational continuity

1.2 Scope

These procedures apply to:

- All exchange partner relationships (OKX, Binance, Bybit, Hyperliquid, and any future venue)
- All personnel involved in trading operations, technology, and management
- All trading accounts, API connections, and fund flows
- All jurisdictions in which the Firm operates or transacts

1.3 Definitions

Term	Definition
AML	Anti-Money Laundering - laws, regulations, and procedures to prevent the generation of income through illegal actions
CTF	Counter-Terrorist Financing - measures to prevent the use of financial systems to fund terrorism
CDD	Customer Due Diligence - the process of verifying the identity and assessing the risk profile of a business relationship
EDD	Enhanced Due Diligence - additional verification measures applied to higher-risk relationships
KYC	Know Your Customer - identity verification procedures
SAR	Suspicious Activity Report - formal report filed when suspicious activity is detected
STR	Suspicious Transaction Report - report filed for specific suspicious transactions
PEP	Politically Exposed Person - an individual entrusted with a prominent public function
UBO	Ultimate Beneficial Owner - the natural person(s) who ultimately own or control a legal entity
FATF	Financial Action Task Force - intergovernmental body setting

	AML/CTF standards
VASP	Virtual Asset Service Provider - as defined by FATF Recommendation 15
ML/TF	Money Laundering / Terrorist Financing
MLRO	Money Laundering Reporting Officer

2. Regulatory Framework & Obligations

2.1 Applicable Regulations & Standards

Framework	Jurisdiction	Relevance
FATF Recommendations	International	Global AML/CTF standards; Recommendation 15 (VASPs); Travel Rule (Rec. 16)
FATF Guidance on VASPs	International	Specific guidance on virtual asset risk assessment and supervision
Hong Kong AMLO	Hong Kong SAR	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
SFC AML/CTF Guidelines	Hong Kong SAR	Securities and Futures Commission guidelines for licensed entities
HKMA Guidelines	Hong Kong SAR	Hong Kong Monetary Authority AML/CTF guidance
EU MiCA	European Union	Markets in Crypto-Assets Regulation; relevant for EU-licensed exchange partners
BSA/AML	United States	Bank Secrecy Act; relevant where US persons or US-based exchanges are involved
OFAC Sanctions	United States	Office of Foreign Assets Control sanctions lists
EU Sanctions Lists	European Union	Consolidated EU sanctions screening
UN Sanctions Lists	International	UN Security Council consolidated list

2.2 The Firm's Regulatory Posture

Formatnull Ventures operates as a proprietary trading firm. While the Firm may not be directly regulated as a VASP in all jurisdictions, it voluntarily adopts FATF-compliant AML/CTF procedures for the following reasons:

6. **Exchange partner requirements**: Major exchanges require institutional counterparties to demonstrate AML compliance
7. **Reputational risk management**: Maintaining institutional-grade compliance protects the Firm's standing
8. **Investor due diligence**: Prospective investors require evidence of robust compliance infrastructure
9. **Regulatory preparedness**: The global regulatory landscape for crypto is evolving rapidly; proactive compliance reduces transition risk
10. **Counterparty confidence**: Robust AML procedures strengthen relationships with banking partners, prime brokers, and custodians

3. Governance & Organizational Structure

3.1 Compliance Governance

Role	Responsibility	Personnel
Managing Partner / Compliance Officer	Ultimate accountability for AML/CTF compliance; policy approval; regulatory liaison	Joshua
Money Laundering Reporting Officer (MLRO)	Receiving and evaluating internal suspicious activity reports; filing SARs with authorities; maintaining SAR register	Managing Partner (interim)
Compliance Analyst	Day-to-day transaction monitoring; CDD/EDD execution; screening; record keeping	Operations Team
Trading Operations	First line of defense; report suspicious patterns; adhere to compliance procedures	All Trading Personnel

3.2 Three Lines of Defense

Line	Function	Responsibility
First Line	Trading Operations & Technology	Identify and report suspicious activity; adhere to AML procedures; maintain trading records
Second Line	Compliance & Risk Management	Policy development; transaction monitoring; CDD/EDD; sanctions screening; training
Third Line	Independent Audit	Periodic independent review of AML/CTF program effectiveness

3.3 Reporting Lines

```
Managing Partner / Compliance Officer
        │
        ├── MLRO (currently: Managing Partner)
        │     └── SAR filing, regulatory reporting
        │
        ├── Compliance Analyst(s)
        │     └── CDD/EDD, screening, monitoring
        │
        └── Trading Operations
              └── First-line identification & reporting
```

4. Risk Assessment Methodology

4.1 Enterprise-Wide Risk Assessment

The Firm conducts a comprehensive ML/TF risk assessment at least annually, evaluating risks across four dimensions:

Dimension	Risk Factors Assessed
Customer/Counterparty	Exchange partner regulatory status, jurisdiction, ownership structure, AML program maturity
Product/Service	Cryptocurrency types traded, leverage products, cross-chain transactions, privacy coins
Geographic	Jurisdictions of exchange partners, server locations, banking relationships
Delivery Channel	API-based trading (higher automation risk), remote access, cross-border data flows

4.2 Risk Scoring Matrix

Each exchange partner relationship is scored across the following criteria:

Factor	Low Risk (1)	Medium Risk (2)	High Risk (3)
Regulatory Status	Fully licensed & regulated in Tier 1 jurisdiction	Licensed in one jurisdiction, pending in others	Unlicensed or licensed in non-FATF jurisdiction
AML Program	Published, audited AML program; SOC 2 Type II	Published AML policy; no independent audit	No published AML policy or unclear compliance
Jurisdiction	FATF member, low-risk (US, EU, JP, HK, SG)	FATF member, medium-risk	FATF grey/black list; high-risk jurisdiction
Proof of Reserves	Regular third-party PoR audits	Self-reported reserves; partial transparency	No PoR; opaque reserve management
Sanctions Compliance	Demonstrated sanctions screening; OFAC compliant	Policy exists; implementation unclear	No sanctions screening; blocked jurisdiction leakage
Track Record	5+ years operation; no material regulatory actions	2–5 years; minor regulatory issues	<2 years; material regulatory actions or hacks
Ownership & UBO	Transparent corporate structure; known UBOs	Partially disclosed ownership	Opaque ownership; nominee structures; PEP involvement
Insurance & Custody	Insured custody; qualified custodian; segregated funds	Partial insurance; co-mingled funds	No insurance; hot wallet dominant; co-mingled

Risk Classification:

- **Score 8–12:** Low Risk - standard CDD
- **Score 13–18:** Medium Risk - enhanced monitoring
- **Score 19–24:** High Risk - EDD required; senior management approval

4.3 Inherent Risk Factors for Crypto Trading Firms

Risk Factor	Description	Mitigation
Pseudonymity	Blockchain addresses are pseudonymous	Exchange-level KYC; withdrawal address monitoring
Cross-Border Velocity	Funds move globally in minutes	Transaction monitoring; jurisdiction-aware limits
Fragmentation	Multiple exchanges and blockchains	Consolidated transaction monitoring across venues
Funding Rate Arbitrage	Complex flow patterns may resemble structuring	Document legitimate trading strategies
High-Frequency Trading	Volume/velocity may trigger exchange AML alerts	Pre-register HFT activity with exchange compliance
API-Based Access	Reduced human oversight per transaction	Automated monitoring; anomaly detection

5. Customer Due Diligence (CDD) — Exchange Partners

5.1 Pre-Onboarding Assessment

Before establishing a trading relationship with any exchange, the Firm conducts the following CDD:

5.1.1 Exchange Identity Verification

- ☐ **Legal entity name** and registration number confirmed via corporate registry
- ☐ **Jurisdiction of incorporation** verified through official registry search
- ☐ **Operating licenses** - copies obtained and independently verified with relevant regulator
- ☐ **Registered office address** confirmed
- ☐ **Website and domain** - WHOIS verification; SSL certificate validation
- ☐ **Contact information** - verified through independent channels (not exchange-provided)

5.1.2 Ownership & Control Structure

- ☐ **Corporate structure chart** obtained showing all entities to ultimate beneficial owners (UBOs)
- ☐ **UBO identification** - all natural persons owning ≥10% identified and verified
- ☐ **PEP screening** - all UBOs and senior management screened against PEP databases
- ☐ **Sanctions screening** - all UBOs, directors, and senior management screened against OFAC, EU, UN, and local sanctions lists
- ☐ **Adverse media screening** - comprehensive search for regulatory actions, fraud, security breaches, or negative press
- ☐ **Shareholder verification** - where possible, verified through independent company registry searches

5.1.3 AML/CTF Program Assessment

- ☐ **AML/CTF policy** - copy obtained and reviewed for adequacy
- ☐ **KYC procedures** - documented and assessed for FATF compliance
- ☐ **Transaction monitoring** - capabilities assessed (real-time vs. batch; rule-based vs. ML)
- ☐ **SAR filing history** - where available, assessed for regulatory engagement
- ☐ **Compliance staffing** - headcount and qualifications of compliance team assessed
- ☐ **Training program** - frequency and content of AML training reviewed
- ☐ **Independent audit** - results of most recent AML audit obtained (if available)
- ☐ **Sanctions screening technology** - vendor and update frequency confirmed
- ☐ **Travel Rule compliance** - readiness assessed for FATF Recommendation 16

5.1.4 Financial Stability Assessment

- ☐ **Proof of Reserves (PoR)** - most recent third-party audit obtained
- ☐ **Insurance coverage** - details of custody/crime insurance reviewed
- ☐ **Fund segregation** - customer fund separation policy assessed
- ☐ **Banking relationships** - primary banking partners identified (indicates regulatory acceptance)
- ☐ **Audited financial statements** - where available, reviewed for going concern risks

5.2 Ongoing Due Diligence

CDD is not a one-time exercise. The Firm conducts ongoing due diligence on all exchange partners:

Activity	Frequency	Responsible
Sanctions screening refresh	Monthly	Compliance Analyst
Adverse media monitoring	Continuous (automated alerts)	Compliance Analyst
Regulatory status verification	Quarterly	Compliance Officer
PoR audit review	Per publication (typically quarterly)	Compliance Analyst
CDD file refresh	Annually (minimum)	Compliance Officer
Risk score recalculation	Annually or upon trigger event	Compliance Officer
Exchange security incident review	Upon occurrence	Compliance Officer + CTO

5.3 Trigger Events for CDD Refresh

The following events trigger an immediate CDD refresh regardless of the scheduled cycle:

- Exchange experiences a security breach or hack
- Exchange receives a regulatory enforcement action
- Change in exchange ownership or UBO structure
- Exchange enters a new or withdraws from a jurisdiction
- Significant change in exchange's AML/CTF policies
- Adverse media report of material concern
- Change in FATF grey/black list status for exchange jurisdiction
- Anomalous transaction patterns detected on the exchange
- Exchange de-banks (loses banking relationship)
- Material market event affecting exchange solvency (e.g., peer exchange collapse)

6. Enhanced Due Diligence (EDD) Procedures

6.1 EDD Triggers

EDD is required when any of the following conditions exist:

Trigger	EDD Requirement
Exchange risk score ≥ 19	Full EDD package
Exchange operates in FATF grey/black list jurisdiction	Geographic EDD
Exchange has UBOs who are PEPs	PEP-specific EDD
Exchange has experienced regulatory enforcement	Regulatory EDD
Exchange has been subject to significant security breach	Security EDD
Unusual transaction patterns detected	Transaction EDD
Exchange is newly established (< 2 years)	New entity EDD

6.2 EDD Procedures

In addition to standard CDD, EDD includes:

6.2.1 Senior Management Approval

- Any high-risk exchange relationship requires **written approval from the Managing Partner** before onboarding or continuation
- Approval must document the rationale for maintaining the relationship and additional risk mitigants

6.2.2 Source of Funds / Source of Wealth

- Verify the exchange's capitalization sources
- Assess the exchange's revenue model and fee structures
- Where possible, obtain audited financial statements

6.2.3 Enhanced Transaction Monitoring

- Reduce monitoring thresholds by 50% for transactions involving high-risk exchanges
- Implement real-time alerts for transfers exceeding $10,000 equivalent
- Daily reconciliation of all fund movements with high-risk counterparties

6.2.4 On-Site Due Diligence (Where Feasible)

- Virtual or physical visit to the exchange's offices
- Meeting with compliance leadership
- Review of technology infrastructure and security controls
- Assessment of operational resilience and business continuity planning

6.2.5 Third-Party Intelligence

- Commission independent due diligence report from a recognized compliance consultancy

- Obtain credit bureau and litigation search reports
- Review of the exchange's relationships with law enforcement (cooperation track record)

6.3 EDD Review Frequency

High-risk relationships subject to EDD are reviewed at minimum **every six months**, or immediately upon trigger event occurrence.

7. Know Your Customer (KYC) — Internal Participants

7.1 Personnel KYC

All individuals with access to trading systems, API keys, or fund management undergo KYC verification:

Requirement	Detail
Identity Verification	Government-issued photo ID (passport or national ID)
Proof of Address	Utility bill or bank statement dated within 3 months
PEP Screening	Screened against international PEP databases
Sanctions Screening	Screened against OFAC SDN, EU, UN consolidated lists
Criminal Background	Self-declaration; independent verification where required by law
Adverse Media	Media search for regulatory/legal issues
Ongoing Monitoring	Annual rescreening of all personnel

7.2 Access Controls

System	Access Level	Authorization Required
Exchange Trading APIs	Restricted	Managing Partner + second approver
Fund Transfer / Withdrawal	Restricted	Managing Partner (sole authority)
Trading Engine Configuration	Operations	Operations Lead approval
Monitoring & Read-Only	Standard	Team lead approval
Compliance Systems	Restricted	Compliance Officer

7.3 API Key Security

- All exchange API keys stored exclusively in **encrypted Kubernetes Secrets** - never in source code, configuration files, or environment variables outside the secure orchestration layer
- API keys configured with **minimum necessary permissions** (trade-only; no withdrawal capability where exchange supports it)
- **IP whitelisting** enabled for all API keys, restricted to the Firm's trading server public IP addresses
- API key rotation schedule: **every 90 days** or immediately upon personnel change
- Emergency API key revocation procedure documented and tested quarterly

8. Transaction Monitoring

8.1 Automated Monitoring Framework

The Firm operates a multi-layered transaction monitoring system:

Layer	Technology	Purpose
Real-Time	Prometheus + Custom Rules	Immediate alerting on threshold breaches
Near-Real-Time	Automated Scripts + Loki Logs	Pattern detection across trading sessions
Periodic	Daily Reconciliation Reports	End-of-day comprehensive review
Ad Hoc	Manual Investigation	Triggered by alerts or external reports

8.2 Monitoring Rules

Rule	Threshold	Action
Large Value Transfer	Single transfer > $50,000 equivalent	Alert; document business purpose
Structuring Detection	Multiple transfers < threshold within 24h summing > $50,000	Alert; investigate for structuring
Unusual Timing	Fund movements outside business hours or during off-hours sessions	Alert; verify authorization
New Counterparty	First transaction with a new address or entity	Alert; verify against approved list
Velocity Alert	>5 fund movements in 24h	Alert; investigate pattern
Cross-Exchange Movement	Funds moved between exchanges without clear trading rationale	Alert; document business purpose
Deviation from Profile	Transaction size > 3σ from rolling average	Alert; investigate anomaly
Withdrawal to Unverified Address	Any withdrawal to a non-whitelisted address	Block; require manual approval
Privacy Coin Interaction	Any inbound transaction involving mixers, tumblers, or privacy coins	Block; escalate to MLRO
Sanctioned Jurisdiction	Any counterparty or address linked to sanctioned jurisdiction	Block; file SAR

8.3 Trading Activity Monitoring

In addition to fund movement monitoring, the Firm monitors trading activity for potential market manipulation or abusive practices:

Pattern	Detection Method	Action
Wash Trading	Self-trade detection across accounts	Alert; investigate
Spoofing/Layering	Order placement/cancellation pattern analysis	Alert; investigate

Front-Running	Correlation between own signals and pre-positioned orders	Alert; investigate
Unusual P&L	Returns > 5σ from expected distribution	Alert; verify signal integrity
Volume Anomalies	Trading volume > 200% of daily average without market event	Alert; document

8.4 Reconciliation Schedule

Reconciliation	Frequency	Content
Position Reconciliation	Real-time (continuous)	Ember OMS positions vs. exchange-reported positions
Fund Balance Reconciliation	Daily (end-of-day)	Internal ledger vs. exchange balances for all venues
Fee Reconciliation	Weekly	Calculated fees vs. exchange-reported fees
P&L Reconciliation	Daily	Strategy PnL vs. accounting records
Comprehensive Audit Trail	Monthly	Full transaction log review with compliance sign-off

9. Suspicious Activity Reporting (SAR)

9.1 Internal Reporting Procedure

Any personnel who identifies or suspects money laundering, terrorist financing, or other financial crime must:

11. **Do not** alert the subject of the suspicion ("tipping off" is a criminal offense in most jurisdictions)
12. **Document** the suspicious activity in detail, including:

- Date, time, and nature of the suspicious activity
- Parties involved (accounts, addresses, entities)
- Why the activity is considered suspicious
- Any supporting evidence (screenshots, logs, transaction IDs)

13. **Report** immediately to the MLRO via the designated secure channel
14. **Do not** proceed with any related transactions until the MLRO provides clearance
15. **Maintain** strict confidentiality about the report

9.2 MLRO Assessment

Upon receiving an internal report, the MLRO will:

16. **Acknowledge** receipt within 24 hours
17. **Assess** the report against the suspicious activity indicators (Appendix C)
18. **Investigate** by gathering additional information as needed
19. **Determine** whether the suspicion is substantiated
20. **File** a SAR with the appropriate regulatory authority if suspicion is substantiated
21. **Document** the decision and rationale regardless of outcome
22. **Update** the SAR register

9.3 SAR Filing

Element	Requirement
Filing Authority	Joint Financial Intelligence Unit (JFIU) - Hong Kong; or FinCEN (US), FIU (EU) as applicable
Filing Timeline	Within 3 business days of MLRO determination
Filing Format	As prescribed by the relevant authority
Confidentiality	SARs are strictly confidential; existence must not be disclosed to any party other than regulators
Record	Filed SAR retained for minimum 7 years

9.4 SAR Register

The MLRO maintains a SAR register containing:

- Unique reference number
- Date of internal report
- Date of MLRO assessment
- Outcome (SAR filed / no SAR filed with rationale)

- Date SAR filed (if applicable)
- Authority filed with
- Follow-up actions
- Status (open / closed)

10. Sanctions Screening

10.1 Screening Scope

All of the following are screened against applicable sanctions lists:

Subject	Screening Point	Frequency
Exchange partner entities	Onboarding + ongoing	Monthly
Exchange UBOs and directors	Onboarding + ongoing	Monthly
Internal personnel	Onboarding + ongoing	Annually
Counterparty wallet addresses	Pre-transaction	Real-time
Incoming deposits	On receipt	Real-time

10.2 Sanctions Lists

List	Source	Update Frequency
OFAC SDN List	US Treasury	Daily
OFAC Non-SDN Lists	US Treasury	Daily
EU Consolidated Sanctions	European Commission	Upon publication
UN Security Council	United Nations	Upon publication
HK Designated Persons	Hong Kong Government	Upon publication
FATF High-Risk Jurisdictions	FATF	Semi-annual publication
Chainalysis / Elliptic Risk Data	Blockchain analytics provider	Continuous

10.3 Screening Procedure

23. **Initial Screen:** Conducted at onboarding using automated name/entity matching
24. **Ongoing Screen:** Automated monthly re-screening against updated lists
25. **Transaction Screen:** Real-time blockchain analytics screening for inbound/outbound transactions
26. **Match Handling:**

- **Exact match:** Immediately freeze activity; escalate to MLRO
- **Potential match (fuzzy):** Investigate within 24 hours; escalate if confirmed
- **False positive:** Document rationale for clearance; retain in screening log

27. **Blocked Jurisdictions:** No trading activity, fund transfers, or counterparty relationships involving:

- North Korea (DPRK)
- Iran
- Syria
- Cuba
- Crimea region
- Any jurisdiction currently on FATF black list

- Any jurisdiction subject to comprehensive OFAC sanctions

11. Record Keeping

11.1 Retention Requirements

Record Type	Retention Period	Storage
CDD/EDD files (exchange partners)	7 years after relationship end	Encrypted digital storage (PostgreSQL + file system)
KYC files (internal personnel)	7 years after departure	Encrypted digital storage
Transaction records	7 years from transaction date	TimeBase + PostgreSQL
Trading logs	7 years from trade date	TimeBase + archived CSV
SAR files and register	7 years from filing date	Encrypted, restricted access
Sanctions screening logs	5 years from screening date	PostgreSQL
Training records	5 years from training date	Digital storage
Risk assessments	7 years from assessment date	Encrypted digital storage
Compliance meeting minutes	7 years from meeting date	Digital storage
Internal correspondence re: compliance	5 years	Digital storage

11.2 Data Protection

- All compliance records stored with AES-256 encryption at rest
- Access restricted to Compliance Officer and MLRO on a need-to-know basis
- Backup copies maintained in geographically separate location
- Data retention automated; destruction logged with compliance sign-off
- Compliance data stored separately from trading data with distinct access controls

12. Training & Awareness

12.1 Training Program

Training	Audience	Frequency	Content
AML/CTF Foundation	All personnel	Upon joining + annually	ML/TF risks, red flags, reporting obligations, sanctions
Exchange-Specific AML	Trading operations	Semi-annually	Venue-specific AML requirements, API constraints, KYC obligations
Advanced Compliance	Compliance team	Quarterly	Regulatory updates, case studies, screening technology
MLRO Training	MLRO	Annually	SAR filing, regulatory liaison, investigation techniques
Incident Response	All personnel	Annually	Escalation procedures, kill switch, evidence preservation

12.2 Training Records

All training completion is documented with:

- Training date and duration
- Trainer / provider
- Attendees
- Training content summary
- Assessment results (where applicable)
- Certificates (where issued)

13. Independent Audit & Review

13.1 Internal Compliance Review

Review	Frequency	Scope
AML program effectiveness	Annually	Full program review against FATF standards
Transaction monitoring effectiveness	Semi-annually	Alert quality, false positive rate, coverage
CDD file quality	Annually	Sample review of exchange partner files
Training effectiveness	Annually	Personnel knowledge assessment
Record keeping compliance	Annually	Retention, accessibility, completeness

13.2 External Independent Audit

- **Frequency:** Every 2 years (minimum) or annually for high-risk periods
- **Scope:** Full AML/CTF program including policies, procedures, monitoring, screening, training, and governance
- **Provider:** Qualified external compliance auditor or consulting firm with virtual asset expertise
- **Output:** Written audit report with findings, recommendations, and remediation timeline
- **Distribution:** Managing Partner, Compliance Officer, external counsel (if applicable)

14. Exchange-Specific Due Diligence Profiles

14.1 OKX

Factor	Assessment	Risk Score
Regulatory Status	Licensed by Dubai VARA; registered in Seychelles; MiCA-compliant EU entity; HK VASP license (pending)	1 (Low)
AML Program	Published compliance framework; dedicated compliance team; Chainalysis integration	1 (Low)
Jurisdiction	Dubai (VARA), Seychelles, Malta	2 (Medium)
Proof of Reserves	Monthly PoR published; third-party audited	1 (Low)
Sanctions Compliance	OFAC-compliant; geo-blocks restricted jurisdictions; wallet screening	1 (Low)
Track Record	7+ years operation; no material regulatory enforcement	1 (Low)
Ownership	Founded by Star Xu; corporate structure disclosed	2 (Medium)
Insurance/Custody	Cold storage majority; insurance on hot wallet; fund segregation	1 (Low)
Overall Risk Score	10 / 24	Low Risk
CDD Level	Standard CDD	

14.2 Binance

Factor	Assessment	Risk Score
Regulatory Status	Multiple licenses globally (Dubai, France, Japan, etc.); US entity (Binance.US) separate; DOJ settlement (2023)	2 (Medium)
AML Program	Significantly enhanced post-DOJ settlement; independent compliance monitor appointed; industry-leading blockchain analytics	1 (Low)
Jurisdiction	Cayman Islands (HQ); global operations	2 (Medium)
Proof of Reserves	Regular PoR published; Mazars engagement (2022-2023)	1 (Low)
Sanctions Compliance	Enhanced post-settlement; comprehensive sanctions screening; OFAC compliance	1 (Low)
Track Record	7+ years; DOJ settlement in 2023 ($4.3B); compliance monitor through 2028	2 (Medium)
Ownership	Founded by Changpeng Zhao; stepped	2 (Medium)

	down as CEO; new CEO Richard Teng	
Insurance/Custody	SAFU fund; cold storage; segregated user funds	1 (Low)
Overall Risk Score	12 / 24	Low Risk
CDD Level	Standard CDD with enhanced monitoring	

14.3 Bybit

Factor	Assessment	Risk Score
Regulatory Status	Licensed in Dubai (VARA); registered in BVI; expanding regulatory footprint	2 (Medium)
AML Program	Published compliance framework; KYC/KYB requirements; blockchain analytics	2 (Medium)
Jurisdiction	BVI (registered); Dubai (operational HQ)	2 (Medium)
Proof of Reserves	PoR published; Hacken audit	1 (Low)
Sanctions Compliance	Geo-blocking; sanctions screening; compliance team	2 (Medium)
Track Record	5+ years; Feb 2025 security incident ($1.4B ETH theft; user funds recovered)	3 (High)
Ownership	Founded by Ben Zhou; corporate structure partially disclosed	2 (Medium)
Insurance/Custody	Cold storage; recovery from Feb 2025 incident demonstrated resilience	2 (Medium)
Overall Risk Score	16 / 24	Medium Risk
CDD Level	Enhanced monitoring; quarterly review	

14.4 Hyperliquid

Factor	Assessment	Risk Score
Regulatory Status	Decentralized exchange; no regulatory license; operates as DeFi protocol	3 (High)
AML Program	Limited centralized AML; relies on on-chain transparency	3 (High)
Jurisdiction	Unclear; decentralized governance	3 (High)
Proof of Reserves	On-chain verifiable (inherent to DEX model)	1 (Low)
Sanctions Compliance	Limited centralized screening; OFAC compliance unclear	3 (High)
Track Record	2+ years; novel protocol; limited track record	3 (High)

Ownership	Pseudonymous team; decentralized governance	3 (High)
Insurance/Custody	Self-custody model (user retains custody)	1 (Low)
Overall Risk Score	20 / 24	High Risk
CDD Level	EDD required; senior management approval; reduced exposure limits	

15. Incident Response & Escalation

15.1 Escalation Matrix

Severity	Definition	Response Time	Escalation
Critical	Confirmed sanctions match; confirmed ML/TF activity; regulatory inquiry	Immediate (< 1 hour)	MLRO → Managing Partner → External Counsel
High	Potential sanctions match; suspicious activity exceeding threshold; exchange security breach	< 4 hours	Compliance Analyst → MLRO → Managing Partner
Medium	Unusual transaction pattern; CDD gap identified; minor compliance deviation	< 24 hours	Compliance Analyst → MLRO
Low	Administrative compliance item; training overdue; record keeping deficiency	< 5 business days	Compliance Analyst

15.2 Incident Response Procedure

28. **Detection:** Alert generated (automated or manual identification)
29. **Triage:** Classify severity per matrix above
30. **Containment:** If trading-related, consider activity suspension; preserve evidence
31. **Investigation:** Gather all relevant data; document findings
32. **Reporting:** File SAR if applicable; notify MLRO
33. **Resolution:** Implement corrective measures
34. **Post-Incident:** Update procedures; conduct lessons-learned review
35. **Documentation:** Complete incident report; update compliance register

15.3 Evidence Preservation

In any compliance incident:

- **Do not delete** any logs, records, or communications
- Capture **timestamped screenshots** of relevant systems
- Export **transaction records** from all relevant exchanges
- Preserve **API logs** from the trading infrastructure (TimeBase, Ember OMS logs retained in Loki)
- Store all evidence in the designated secure compliance directory with access logging

16. Policy Review & Amendment

16.1 Review Schedule

Review Type	Frequency	Owner
Full policy review	Annually	Managing Partner
Regulatory update assessment	Quarterly	Compliance Officer
Risk assessment refresh	Annually (or upon trigger)	Compliance Officer
Procedure effectiveness review	Semi-annually	Compliance Officer

16.2 Amendment Process

36. Proposed amendment documented with rationale
37. Impact assessment on existing procedures
38. Review by Compliance Officer
39. Approval by Managing Partner
40. Communication to all affected personnel
41. Training update (if procedural change)
42. Version control update and prior version archived

Appendix A — Risk Assessment Matrix

Country / Jurisdiction Risk Classification

Risk Level	Jurisdictions
Low Risk	United States, United Kingdom, European Union (MiCA jurisdictions), Japan, South Korea, Singapore, Hong Kong, Australia, Canada, Switzerland
Medium Risk	UAE (Dubai/VARA), Bermuda, Cayman Islands, BVI, Mauritius, Turkey, Brazil, India
High Risk	FATF Grey List jurisdictions (current list: [refer to latest FATF publication])
Prohibited	FATF Black List; OFAC comprehensively sanctioned: North Korea, Iran, Syria, Cuba, Crimea/Donetsk/Luhansk regions

Appendix B — Due Diligence Questionnaire (DDQ)

The following questionnaire is provided to exchange partners during the CDD process:

Section 1: Entity Information

43. Full legal name of the entity
44. Registration number and jurisdiction of incorporation

45. Registered office address
46. Date of incorporation
47. Nature of business and services offered
48. Names and nationalities of all directors
49. Ultimate Beneficial Owners (all persons holding ≥10%)
50. Organization chart showing corporate structure

Section 2: Regulatory & Compliance

51. List all regulatory licenses held (jurisdiction, regulator, license number, date issued)
52. Has the entity or any director/UBO been subject to regulatory enforcement? (Details)
53. Describe your AML/CTF compliance program
54. Name and qualifications of your Chief Compliance Officer / MLRO
55. Do you conduct independent AML program audits? (Frequency, most recent date)
56. Describe your KYC / customer identification procedures
57. Describe your transaction monitoring systems and capabilities
58. Describe your sanctions screening process and technology
59. Are you Travel Rule compliant? (Technology provider used)
60. Describe your SAR/STR filing process

Section 3: Security & Custody

61. Describe your fund custody arrangements (hot/cold ratio, custodian details)
62. Do you maintain Proof of Reserves? (Frequency, auditor)
63. Describe your cybersecurity framework and certifications (SOC 2, ISO 27001, etc.)
64. Have you experienced any security breaches? (Details and remediation)
65. Describe your business continuity and disaster recovery plans
66. Do you maintain insurance coverage? (Type, coverage amount, insurer)

Section 4: Operations

67. Describe your market surveillance capabilities
68. How do you handle market manipulation detection?
69. Do you support institutional API access with IP whitelisting?
70. Describe your API key permission model (trade-only, withdrawal, etc.)
71. What is your incident notification procedure for security events?
72. Do you have a dedicated institutional / OTC desk or relationship management?

Appendix C — Suspicious Activity Indicators

Indicators Related to Fund Movements

- Rapid movement of funds between multiple exchanges without apparent trading purpose
- Deposits immediately followed by withdrawals of equivalent amount ("pass-through")
- Use of multiple wallet addresses to structure transactions below reporting thresholds
- Transactions involving addresses linked to known darknet markets, mixers, or tumblers
- Unexplained receipt of funds from unknown or unverified sources
- Transactions inconsistent with the stated nature of business

Indicators Related to Trading Activity

- Trading patterns that appear designed to generate artificial volume (wash trading)
- Rapid placement and cancellation of large orders (spoofing/layering)
- Trading concentrated in illiquid or newly listed tokens with no fundamental rationale
- Unusual profit patterns inconsistent with stated strategy methodology
- Use of multiple accounts to circumvent position limits or other controls

Indicators Related to Counterparties

- Counterparty reluctant to provide CDD documentation
- Counterparty uses nominee structures without clear business purpose
- Counterparty has connections to high-risk jurisdictions without clear explanation
- Changes in counterparty ownership or control structure without notification
- Counterparty's transaction profile inconsistent with their stated business model

Indicators Related to Exchange Partners

- Exchange suspends withdrawals without adequate explanation
- Exchange experiences unexplained changes in leadership
- Exchange removes or weakens KYC requirements
- Exchange begins supporting privacy coins or mixing services without updated compliance measures
- Exchange's geographic blocking appears inconsistent (IP-only without KYC-level geo checks)

Appendix D — Document Retention Schedule

Document Category	Retention Period	Destruction Method
CDD/EDD Files	7 years post-relationship	Secure digital deletion with certification
KYC Records	7 years post-departure	Secure digital deletion with certification
Transaction Records	7 years post-transaction	Secure digital deletion with certification
SARs and SAR Register	7 years post-filing	Secure digital deletion with certification
Sanctions Screening Logs	5 years post-screening	Secure digital deletion
Training Records	5 years post-training	Secure digital deletion
Risk Assessments	7 years post-assessment	Secure digital deletion with certification
Compliance Meeting Minutes	7 years post-meeting	Secure digital deletion
Incident Reports	7 years post-incident	Secure digital deletion with certification
Policy Versions	Indefinite (all versions)	N/A - permanent archive
Internal Audit Reports	7 years post-report	Secure digital deletion with certification
External Audit Reports	7 years post-report	Secure digital deletion with certification

Appendix E — Approval & Sign-Off Sheet

Document Control

Version	Date	Author	Changes	Approved By
1.0	May 1, 2026	Joshua Hall	Initial release	Joshua Hall, Managing Partner

Acknowledgment

By signing below, I confirm that I have read, understood, and agree to comply with the Formatnull Ventures AML & Due Diligence Procedures.

Name	Role	Signature	Date

Formatnull Ventures

Compliance & Risk Division

Email: compliance@formatnull.com

This document contains proprietary and confidential information belonging to Formatnull Ventures. Unauthorized reproduction, distribution, or disclosure is strictly prohibited. This document does not constitute legal advice and should be supplemented by guidance from qualified legal counsel in relevant jurisdictions.

Legal Notice: This policy is intended as an operational compliance framework and does not constitute legal advice. Formatnull Ventures should supplement this document with jurisdiction-specific advice from qualified legal counsel where required.