

CRYPTO RISK MANAGEMENT POLICY AND PROCEDURES (GCB)

Deep Dive Tech BV

Document Type	Policy Owner	Approved by	Version	Effective Date	Next Review Date
Policy & Standard Operating Procedures (SOP)	Compliance Department (MLRO / Head of Compliance)	Board of Directors	1.0	01/08/2025	01/08/2026

Applies to: All Deep Dive Tech B.V. staff, contractors, and third parties involved in cryptocurrency ("crypto") processing, including PSPs, VASPs, custodians, and analytics providers.

Contents

- 1. Purpose & Objectives 3
- 2. Scope..... 3
- 3. Definitions (Key Terms)..... 3
- 4. Regulatory & Standards Alignment 4
- 5. Governance, Roles & Responsibilities 5
- 6. Risk Appetite & Control Standards 6
 - 6.1. Asset Acceptance Standard 6
 - 6.2. Monitoring & Screening 6
 - 6.3. Thresholds & Escalation (Examples)..... 6
- 7. Vendor & Third-Party Management 7
- 8. Monitoring, Alerts & Reporting 7
- 9. Training & Awareness 7
- 10. Record Keeping..... 7
- 11. Review & Approval 8

1. Purpose & Objectives

This Policy and its Procedures establish Deep Dive Tech B.V.'s framework to identify, assess, mitigate, monitor, and report risks arising from the acceptance, transfer, conversion, and withdrawal of cryptocurrency in connection with online gaming operations. Objectives:

- i. Ensure compliance with the Curaçao Gaming Control Board ("GCB") expectations and applicable AML/CFT obligations.
- ii. Prevent and detect money laundering, terrorism financing, fraud, and sanctions evasion through the use of crypto.
- iii. Protect customers and the Company by applying risk-based controls, including on-chain and off-chain monitoring.
- iv. Provide clear, auditable procedures, roles, and evidence for internal/external audits and regulatory assessments.

2. Scope

- i. Activities: Customer deposits, withdrawals, transfers between Company wallets, conversions to/from fiat or stablecoins, and interactions with third-party VASPs/PSPs.
- ii. Assets: Only approved cryptocurrencies and tokens as per Section 6.1 (Asset Acceptance Standard).
- iii. People: All employees/contractors in Compliance, Payments/Finance, IT/Security, Customer Support, and Risk/Fraud.
- iv. Third parties: Crypto PSPs, custodians, liquidity providers, blockchain analytics vendors, and Travel Rule service providers.

3. Definitions (Key Terms)

- Virtual Asset (VA): Digital representation of value that can be digitally traded or transferred, used for payment or investment purposes.
- Virtual Asset Service Provider (VASP): Entity conducting exchange, transfer, safekeeping/administration of VAs, or providing related services.
- On-Chain Monitoring (KYT): Screening/analysis of blockchain transactions/addresses for ML/TF/sanctions risk, using specialist analytics.
- Off-Chain Monitoring: Monitoring of customer behavior, devices, geolocation, velocity and transactional patterns within the platform/PSP.
- Travel Rule: Requirement to transmit originator/beneficiary information alongside VA transfers when applicable.

- Custody Types: Hot wallets (connected), Warm (limited connectivity), Cold (offline). Multi-signature/threshold schemes apply where feasible.

4. Regulatory & Standards Alignment

Deep Dive Tech B.V. aligns this Policy with:

- i. GCB AML/CFT expectations for licenses, including crypto acceptance controls.
- ii. FATF Recommendations (esp. 1, 10, 15, 16) and risk-based approach to VAs/VASPs, as follows:
 - a. Recommendation 1 - Risk-Based Approach (RBA)
 - Countries, financial institutions, and VASPs should identify, assess, and understand ML/TF risks and apply a risk-based approach.
 - Controls and resources should be proportionate to the level of risk.
 - Requires regular national risk assessments and institutional risk assessments.
 - In the VA/VASP context: assess risks from specific virtual assets, delivery channels (e.g., online, P2P), jurisdictions, and customer types.
 - b. Recommendation 2 - Customer Due Diligence (CDD)
 - Requires identifying and verifying the identity of customers and beneficial owners before establishing a business relationship or conducting transactions above a certain threshold.
 - Includes ongoing due diligence and scrutiny of transactions.
 - For VASPs:
 - KYC must be done before customers can deposit or withdraw VAs.
 - Higher thresholds and Enhanced Due Diligence (EDD) apply for high-risk customers or jurisdictions.
 - c. Recommendation 3 - New Technologies
 - Countries and VASPs must assess risks from new technologies (e.g., blockchain, privacy coins, mixers) before launch.
 - Implement controls to mitigate misuse for ML/TF.
 - Explicitly applies to VAs/VASPs since FATF updated this recommendation in 2019.
 - Requires licensing/registration and monitoring of VASPs by competent authorities.

d. Recommendation 4 - Wire Transfers (Travel Rule)

- Requires that originator and beneficiary information be included and transmitted in VA transfers.
- VASPs must collect and securely transmit name, account number (wallet address), and other identifying information when transferring VAs between VASPs or between a VASP and another obliged entity.
- Applies for transactions above the threshold (USD/EUR 1,000 in many jurisdictions) - but regulators may require below this level in high-risk cases.

iii. Applicable local AML/CFT laws and reporting obligations to the Financial Intelligence Unit (FIU).

iv. International sanctions regimes (UN/EU/OFAC/UK), as applicable.

v. Data protection obligations (e.g., GDPR-equivalent where relevant) for personal data used in monitoring.

Note: Where requirements conflict, the Company applies the stricter standard and documents the rationale.

5. Governance, Roles & Responsibilities

MLRO / Board of Directors

- Approves Policy and major changes (e.g., asset acceptance, tooling, risk appetite).
- Receives quarterly crypto risk reports and significant incident notifications.
- Maintains Policy and Procedures; leads risk assessment and control design.
- Approves EDD decisions, high-risk transactions, STR filings to the FIU.
- Oversees vendor due diligence and ongoing monitoring for VASPs/analytics providers.

Payments / Finance

- Operates wallets within approved limits and segregation (hot/warm/cold); manages liquidity and conversions.
- Performs daily reconciliation; resolves breaks; retains audit trails.

Risk & Fraud

- Configures behavioural rules (velocity, device, IP, geolocation); investigates alerts with Compliance.

IT & Security

- Maintains key management, access controls (least privilege), HSMs/secure modules; change management.

Customer Support

- Executes customer outreach (KYC refresh, Travel Rule info), follows hold/deny instructions.

Internal Audit / 2nd Line QA

- Performs periodic effectiveness reviews; validates sampling and evidence.

6. Risk Appetite & Control Standards

6.1. Asset Acceptance Standard

- Accept only approved assets (e.g., BTC, ETH, USDT, USDC) following due diligence.
- Maintain a Master Asset Register with network(s), contract addresses, fee settings, risk notes, and de-listing triggers.
- Prefer major stablecoins for settlement; convert customer deposits to stablecoin or fiat currency as soon as operationally feasible to minimise volatility risk, in line with the Company's risk appetite and treasury management procedures.

6.2. Monitoring & Screening

- On-chain (KYT): Deep Dive Tech B.V. only works with CryptoPay as its cryptocurrency payment processor. CryptoPay uses Chainalysis for blockchain transaction monitoring. They screen all incoming and outgoing transactions for risks such as sanctions exposure or illicit activity, based on factors including counterparties, transaction value, and transaction frequency.
- Off-chain: Device/IP/velocity rules, payment patterns, proxy/VPN/TOR use, multi-accounting, bonus abuse, and collusion signals.

6.3. Thresholds & Escalation (Examples)

- Auto-hold transactions where blockchain monitoring indicates a high risk level or confirmed sanctions exposure.
- Manual review for transactions flagged as medium risk or where activity patterns deviate significantly from the customer's usual behaviour.

- iii. Apply Enhanced Due Diligence and seek MLRO approval for large or otherwise high-risk transactions, based on the Company's risk assessment and applicable legal thresholds.

7. Vendor & Third-Party Management

- i. Conduct initial and annual due diligence on VASPs, custodians, PSPs, and analytics providers covering: licensing/registration, sanctions controls, Travel Rule capability, data security, chain coverage, model transparency, uptime/SLA, adverse media, financial soundness.
- ii. Maintain contracts with clear responsibilities (screening scope, alert SLAs, data retention, breach notification, right to audit, sub-processor controls).
- iii. Test vendor outputs quarterly with known test cases (sanctioned, mixer-linked, scam-tagged addresses) and document results.

8. Monitoring, Alerts & Reporting

- i. All crypto transactions are subject to real-time monitoring.
- ii. Alerts generated across on-chain and off-chain systems are routed to a unified case management queue with priority tags.
- iii. Suspicious transactions must be reported to the Compliance Officer immediately.
- iv. Where appropriate, file a Suspicious Transaction Report (STR) with the FIU within the required timeframe.

9. Training & Awareness

- i. Annual training for all relevant staff on crypto-related risks, typologies, and red flags.
- ii. Refresher sessions whenever regulatory updates occur.
- iii. Role-specific training for Payments/Support and Investigations teams.

10. Record Keeping

- i. Maintain all transaction records, customer identification data, and monitoring reports for at least 5 years after the business relationship ends.
- ii. Store monitoring outputs securely; restrict access on a need-to-know basis.

11. Review & Approval

This Policy will be reviewed at least annually or upon significant regulatory changes. Updates must be approved by the Board of Directors.

Signed by:
Signature: Mark Taylor
9ACE813ECC604A9...

MLRO: Mark Taylor