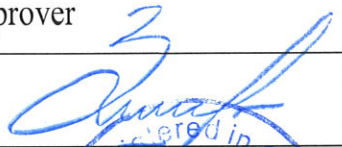


HIGHBET B.V.

Abraham Mendez Chumaceiro Boulevard 03, Willemstad, Curacao
Registration No. 148202
(the “**Company**”)

Crypto Risk Management Policy
(the “**Policy**”)

Version	Status	Date	Comments	Approver
1.0	Approved	24.03.2025	Initial Policy Creation	

Policy Ownership

- **Policy Owner: HighBet B.V.**
- **Created by: Yevhenii Pyroh / MLRO**
- **Approved by: Andrii Zabiaka / Director**
- **Date Approved: 24.03.2025**
- **Last Reviewed: 24.03.2025**
- **Review Frequency: Annual**
- **Next Review Date: 24.09.2025**
- **Security Classification: Private and Confidential**



1. Introduction

HighBet B.V. is committed to maintaining a secure, transparent, and compliant framework for cryptocurrency transactions in its online gaming operations. This policy establishes the risk management framework for cryptocurrency-related risks, including compliance, transaction oversight, operational risk mitigation, cybersecurity, market volatility, AML/CFT controls, and fraud prevention.

2. Scope and Purpose

This policy applies to all cryptocurrency transactions processed by the Company, covering employees, third-party service providers, and partners involved in the handling, monitoring, and processing of such transactions. The objective is to establish a structured risk management framework to identify, assess, and mitigate potential threats arising from cryptocurrency usage, in line with the latest CGA AML requirements.

3. Risk Management Measures

3.1 Business and Customer Risk Assessments

- Business Risk Assessment (BRA) is conducted annually to identify inherent ML/TF risks specific to our operations, markets, products, and technologies.
- Customer Risk Assessment (CRA) is applied to each player and updated periodically. Customers are categorized as Low, Medium, or High risk based on:
 - Source of funds and wealth;
 - Geographic risk;
 - Use of high-risk products or services;
 - Transaction behavior

The Company assesses risks in the following categories:

- **Regulatory & Compliance Risks** – Failure to comply with local and international regulations.
- **Operational Risks** – Transaction failures, security vulnerabilities, human errors.
- **Market Risks** – Cryptocurrency price volatility affecting liquidity.
- **Cybersecurity Risks** – Hacking, phishing, unauthorized access.
- **AML & Fraud Risks** – Money laundering, financial crime, fraudulent transactions.

3.2 Risk Mitigation Strategies

- **Regulatory Compliance:** Regular review of Curaçao, FATF, and EU regulations.
- **Transaction Monitoring:** Real-time risk scoring and compliance escalation.
- **Cybersecurity:** Advanced encryption, 2FA, and cold storage for asset protection.
- **Liquidity Management:** Limiting crypto holdings and fiat conversion mechanisms.
- **Third-Party Risk Management:** Due diligence on exchanges and payment processors.

3.3 Ongoing Risk Monitoring & Adaptation

- Use of AI, blockchain forensics, and compliance analytics.
- Regular assessments based on emerging threats, regulatory updates, and audit findings.
- Dynamic policy updates to reflect best practices and compliance expectations.

3.4 Customer Acceptance Policy (CAP)

The Company maintains a CAP that defines:

- High-risk customer characteristics (e.g., PEPs, crypto whales, irregular activity);
- Risk indicators and levels (Low/Medium/High);
- Triggers for Enhanced Due Diligence (EDD);
- Circumstances under which customer onboarding or continuation is declined;

3.5 Customer Due Diligence (CDD)

CDD is required:

- Upon account registration (basic info collection and screening);
- When financial transactions reach NAf 4,000 (or equivalent);
- When unusual or suspicious behavior is observed;
- For all high-risk players regardless of threshold;

CDD measures include:

- Identification: Name, address, DOB, nationality;
- Verification: Unexpired government ID, proof of address, biometric (if applicable);
- Source of funds and wealth;
- Sanctions screening (UN, EU, OFAC);
- PEP screening (global and local lists);

3.6 Transaction Monitoring and Anomaly Detection

The Company employs real-time monitoring tools to detect irregularities such as:

- High-value transactions or rapid withdrawals.
- Frequent fund movements between multiple accounts.
- Transactions with high-risk or unregulated exchanges.
- Use of privacy-focused cryptocurrencies (Monero, Zcash).

3.7 AML Compliance and Reporting

The AML framework includes:

- All Suspicious Activity Reports (SARs) are filed with FIU Curaçao;

- Tipping-off is strictly prohibited;
- Linked transactions are monitored to detect cumulative thresholds;

3.8 Enhanced Due Diligence (EDD)

EDD is triggered when:

- A player is categorized as high-risk;
- A transaction exceeds standard risk thresholds;

EDD includes:

- Additional documents (e.g., employment proof, bank statements);
- Source of wealth verification;
- Management approval before continuing the relationship;

3.8.1 Simplified Due Diligence (SDD)

SDD may be applied for low-risk customers under strict conditions, such as limited account activity, no international transactions, and no red flags. Identity verification may be deferred but not skipped.

3.9 Cybersecurity and Fraud Prevention

To ensure security:

- End-to-end encryption of transaction data.
- Multi-factor authentication (MFA) for access controls.
- Regular cybersecurity audits.
- AI-driven fraud detection systems (IP monitoring, behavioral analytics).

4. Governance and Policy Review

4.1 Risk Governance Structure

- Board of Directors – Provides strategic oversight, approves risk management policies, and ensures regulatory compliance.
- Compliance Officer – Identifies, assesses, and mitigates cryptocurrency-related risks as well as ensures AML/CFT compliance and escalates suspicious activities to regulators.
- IT Security & Compliance Team – Oversees cybersecurity controls, data protection, and fraud prevention mechanisms.
- Risk Committee – Conducts periodic risk assessments, reviews incidents, and provides recommendations for risk mitigation.

4.2 Independent Risk Audits & Compliance Reviews

- Internal audits are conducted semi-annually to assess risk controls, operational efficiency, and compliance with internal policies.
- External compliance reviews are performed by third-party auditors to validate adherence to regulatory requirements.
- The results of audits are reported to the Board of Directors and Risk Committee, with corrective actions implemented as needed.

4.3 Annual Policy Review & Amendments

- This policy is subject to annual reviews by the Compliance Officer and external compliance advisors.
- Policy updates are made to reflect changes in regulatory frameworks, technological advancements, and industry best practices.
- Amendments are communicated to all employees, and acknowledgment of compliance is mandatory.
- The Board of Directors must approve any significant changes before implementation.

5. Staff Training and Reporting

5.1 Employee Risk Awareness & Training

- All employees involved in cryptocurrency transactions shall undergo mandatory a bi-annual training covering:
 - Transaction monitoring techniques and fraud detection mechanisms.
 - AML compliance obligations and risk mitigation strategies.
 - New and emerging threats in the cryptocurrency industry.
- Employees shall pass periodic assessments to ensure comprehension of risk-related policies.
- Training sessions will be updated regularly to reflect regulatory changes and industry best practices.
- Specialized training will be provided for key personnel such as compliance officers, financial managers and IT security staff.

5.2 Risk Incident Reporting & Escalation

- Employees must immediately report any suspicious activity to the Compliance Officer.

- A formal incident report must be filed, detailing the nature of the risk, individuals involved, and preliminary findings.
- SARs (Suspicious Activity Reports) shall be submitted to FIU Curaçao in cases where financial crime is suspected.
- A whistleblower mechanism is in place to allow employees to report risks anonymously without fear of retaliation.
- All reported incidents will be reviewed by the Risk Committee, and corrective actions will be implemented as necessary.

6. Record-Keeping and Risk Data Management

The Company maintains comprehensive and secure records of all cryptocurrency transactions, risk assessments, and monitoring activities.

Storage and security measures:

- Data is stored in encrypted formats with access controls to prevent unauthorized modifications.
- Blockchain analytics tools are used to trace cryptocurrency transactions and detect illicit activities.
- All records are kept for a minimum of five years in compliance with Curaçao AML regulations.

Regulatory audit compliance:

- Records must be readily available for regulatory audits and compliance reviews.
- A dedicated compliance team ensures that all required documentation is up-to-date.
- Periodic internal and external audits assess the effectiveness of data management processes.

In case of an investigation, transaction records may be shared with law enforcement agencies and regulatory bodies in accordance with legal requirements.

7. Policy Breaches and Disciplinary Actions

Any non-compliance with this Policy may result in immediate disciplinary action, which may include:

- Mandatory re-training for minor breaches.
- Formal warnings and internal reviews for repeated violations.
- Financial penalties for breaches that result in regulatory fines or reputational damage to the Company.
- Employment termination for severe or deliberate non-compliance.

Regulatory Consequences:

- Significant policy violations may lead to mandatory reporting to FIU Curaçao and other regulatory authorities.
- The Company reserves the right to cooperate with law enforcement agencies in cases of fraud, money laundering, or other illegal activities.

Appeals Process:

- Employees subject to disciplinary action may request a formal review.
- The appeal will be reviewed by an independent compliance officer and the Risk Committee.

8. Conclusion

This Crypto Risk Management Policy establishes a structured and proactive approach to identifying, assessing, and mitigating risks associated with cryptocurrency transactions. HighBet B.V. remains committed to continuous improvement in risk management practices, ensuring full compliance with regulatory frameworks and maintaining the highest standards of operational security.