

mBet Solutions N.V.

CRYPTO RISK ASSESSMENT POLICY

v1.0

Version Number	v1
Status	Active
Authorization and approved by	The Director of mBet Solutions N.V.
Review	Annual

Effective date	Version	Comments
07/10/2024	v1	Adoption of the policy

a

Table of Contents

1. Introduction	4
2. Regulatory Framework.....	4
3. Risk Identification.....	6
3.2. Market Risks.....	6
3.3. Cybersecurity Risks.....	6
3.4. Fraud & Financial Crime Risks	7
3.5. Operational Risks	7
3.6. Regulatory Risks	8
4. Risk Matrix.....	9
5. Risk Management Framework	9
5.2. Risk Mitigation Strategies	9
5.2.2. Market Risk Mitigation.....	9
5.2.3. Cybersecurity Risk Mitigation	10
5.2.4. Fraud and Financial Crime Risk Mitigation	10
5.2.5. Operational Risk Mitigation	10
5.2.6. Regulatory Risk Mitigation	11
5.3. Governance and Oversight.....	11
5.3.1. Compliance Officer (CO).....	11
5.3.2. Board of Directors	12
5.4. Incident Management and Response	12
5.5.1. Incident Response Team (IRT)	12
5.5.2. Escalation Procedures	13
5.6. Regular Reviews and Updates	13
6. Compliance and Reporting.....	14
6.1. Internal Reporting:	14
6.2. Regulatory Reporting:.....	14
7. Player Education.....	14
8. Ongoing Monitoring.....	15

1. Introduction

- 1.1. This Crypto Risk Assessment Policy (hereinafter the “Policy”) outlines the framework and processes through which mBet Solutions N.V. (hereinafter the “Company”) assesses, manages, and mitigates risks related to the use of cryptocurrencies in our online gambling operations. The primary focus is on protecting the business from operational, financial, and reputational risks, ensuring compliance with regulatory requirements, and safeguarding players’ interests.
- 1.2. As a holder of a Curacao gambling licence, we are committed to upholding all regulatory obligations in line with the local Know Your Customer (KYC) and Due Diligence (DD) requirements. This Policy complements and must be read in conjunction with our broader Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) policies established at an earlier date.

2. Regulatory Framework

- 2.1. The Policy is designed to comply with a wide range of international, regional, and local regulatory requirements. It ensures that the use of cryptocurrencies in our online gambling operations is conducted in a secure, transparent, and compliant manner. The following key regulatory frameworks and standards are central to our operations.
- 2.2. As a company licensed under the Curacao gambling jurisdiction, we are required to adhere to all guidelines set forth by Curacao’s eGaming regulations.
 - 2.2.1. We are obligated to verify the identity of our players before allowing them to participate in gambling activities, especially when dealing with cryptocurrencies. This process includes collecting sufficient information to identify and verify the player’s name, address, date of birth, and contact details.
 - 2.2.2. To prevent money laundering and terrorist financing, we are required to carry out additional due diligence measures for high-risk customers, including enhanced checks for politically exposed persons (PEPs) and individuals from high-risk jurisdictions.
 - 2.2.3. Continuous monitoring of player activity and transactions is mandatory to detect suspicious or unusual behaviour, including patterns that may indicate fraud, money laundering, or other financial crimes.
 - 2.2.4. In cases of suspicious transactions, we are legally obligated to file Suspicious Transaction Reports (STR) and Suspicious Activity Reports (SAR) with the relevant Curacao Financial Intelligence Unit (FIU).

al

- 2.3. To comply with the AML/CFT standards, we follow the guidelines set by the Financial Action Task Force (FATF), which provides a global framework for combating illicit financial activities.
 - 2.3.1. Our AML/CFT strategy applies a risk-based approach, focusing more resources and controls on higher-risk areas like cryptocurrency transactions. This includes setting stricter monitoring rules for larger or unusual transactions, such as high-volume cryptocurrency trades or players from jurisdictions with weak AML/CFT frameworks.
 - 2.3.2. The Company follows FATF's customer identification procedures, requiring proof of identity, source of funds, and the purpose of the gambling relationship.
 - 2.3.3. Enhanced checks are required for high-risk customers and situations involving cryptocurrencies due to their potential for anonymity and cross-border transfers.
 - 2.3.4. Continuous monitoring of customer transactions ensures we can spot suspicious activity, which might indicate attempts to launder money or finance terrorism.
 - 2.3.5. We integrate global sanctions lists (such as OFAC, EU, UN, etc.) and screen for PEPs to mitigate the risk of doing business with sanctioned individuals or entities.
- 2.4. As the Company also operates in GDPR-compliant regions, we are committed to protecting player data and complying with GDPR requirements.
 - 2.4.1. We collect only the information necessary to meet our KYC, CDD, and AML obligations, ensuring that data collection aligns with GDPR's principles of proportionality and necessity.
 - 2.4.2. Our platforms are built with privacy in mind, ensuring encryption of personal and financial data, particularly when processing cryptocurrency transactions.
 - 2.4.3. We only retain player data for as long as required by law or for the purpose of AML/CFT obligations. Data is securely deleted or anonymized once it is no longer needed.
 - 2.4.4. Players have the right to access, correct, or delete their personal information. They are also informed about their rights to data portability and to lodge complaints with relevant data protection authorities.

3. Risk Identification

3.1. Cryptocurrency use in online gambling introduces a unique set of risks that require careful identification and assessment. This section outlines the key risk categories relevant to our operations, emphasising the importance of understanding how each risk affects our business, players, and regulatory obligations.

3.2. Market Risks

3.2.1. Cryptocurrencies are subject to rapid price fluctuations due to market conditions, investor sentiment, or regulatory news. Significant drops in cryptocurrency value can affect player balances, Company funds, and liquidity.

3.2.1.1. Players may experience substantial losses in the value of their deposits or winnings, leading to dissatisfaction or disputes.

3.2.1.2. If the Company holds cryptocurrency reserves, their value may fluctuate, affecting operational liquidity and long-term financial stability.

3.2.1.3. Some cryptocurrencies may suffer from low liquidity, making it difficult for the Company to quickly convert assets into fiat currencies or other crypto assets, especially in times of high demand or market stress.

3.3. Cybersecurity Risks

3.3.1. The gambling industry is a frequent target of hackers. The nature of cryptocurrencies and the anonymity they offer can attract cybercriminals seeking to steal digital assets.

3.3.1.1. If the Company uses external cryptocurrency exchanges, it is vulnerable to breaches on those platforms, which could result in loss of funds.

3.3.1.2. Hot wallets, which are connected to the internet for quick access to funds, are vulnerable to hacking, potentially leading to large-scale theft.

3.3.1.3. Both the Company and its players are at risk of malware infections or phishing attacks aimed at stealing cryptocurrency keys or gaining unauthorised access to crypto wallets.

- 3.3.2. For companies using decentralised finance (DeFi) platforms or smart contracts to handle certain aspects of cryptocurrency betting or payments, vulnerabilities in the code can be exploited by attackers.

3.4. Fraud & Financial Crime Risks

- 3.4.1. Cryptocurrencies' pseudonymous nature makes them attractive for money laundering activities. Criminals may attempt to:
 - 3.4.1.1. use the platform to deposit illicitly gained funds in the form of cryptocurrencies, converting them into other assets or withdrawing them after use in gambling activities.
 - 3.4.1.2. through complex transactions hide the source of funds by layering, using our platform as an intermediary in their laundering schemes.
- 3.4.2. The anonymity and borderless nature of cryptocurrencies also pose risks of facilitating terrorist financing, where small amounts of funds can be moved quickly and without detection.
- 3.4.3. Players may use stolen cryptocurrency for deposits, leading to disputes when the rightful owners attempt to reclaim funds.
- 3.4.4. Players may initiate fraudulent chargebacks or complaints after using stolen credit cards or compromised payment methods to purchase cryptocurrency.
- 3.4.5. The risk of crypto wallets being compromised, either through social engineering, phishing, or technical exploits, may result in both the Company and players losing access to funds.

3.5. Operational Risks

- 3.5.1. Errors in processing cryptocurrency transactions, either due to system glitches or human error, can lead to failed or delayed payments, which may frustrate players and harm the Company's reputation.
- 3.5.2. Cryptocurrency transactions rely on blockchain networks that may experience congestion during high-volume periods. This can result in:
 - 3.5.2.1. players experiencing slow deposit or withdrawal times, affecting their betting experience.
 - 3.5.2.2. increased fees during network congestion, potentially reducing the amount of crypto players receive during withdrawals.

a

- 3.5.3. The mismanagement of private keys, either through loss or theft, can lead to the permanent loss of funds. Both the Company and players need secure key management systems.
- 3.5.4. If the Company uses third-party custodians for storing cryptocurrency, there is a risk of loss if the custodian is hacked or becomes insolvent.

3.6. Regulatory Risks

- 3.6.1. Failure to comply with AML/CFT regulations in Curacao and other jurisdictions can lead to penalties, fines, or revocation of the gambling licence.
 - 3.6.1.1. Not properly verifying the identity of players, particularly high-risk players, increases the risk of being used for illegal financial activities.
 - 3.6.1.2. Failing to report suspicious transactions or activity to the appropriate authorities in a timely manner can result in regulatory action.
- 3.6.2. As cryptocurrencies evolve, international regulations are continuously changing. A lack of clear, unified regulations across jurisdictions, or international standards (e.g., between Curacao and other countries) can introduce a risks of complexity of such other local laws and requirements.
- 3.6.3. Different jurisdictions have different taxation requirements for cryptocurrency transactions. Failure to correctly report earnings, transactions, or gambling proceeds tied to cryptocurrencies may lead to financial penalties.

a

4. Risk Matrix

Our Risk Matrix assesses risks across the following dimensions:

Risk type	Likelihood	Impact	Risk Level
Market Risks	Medium	High	Medium-High
Cybersecurity Risks	High	Very High	High
Fraud & Financial Crimes	Medium	High	High
Operational Risks	Low	Medium	Low-Medium
Regulatory Risks	Medium	High	High
Reputational Risks	Medium	High	Medium-High

5. Risk Management Framework

5.1. The Risk Management Framework is designed to mitigate the risks associated with cryptocurrency transactions in online gambling. This framework addresses both proactive and reactive strategies, ensuring that the Company can not only prevent potential risks but also respond effectively when issues arise. The framework is based on best practices in risk management and is regularly updated in response to evolving risks and regulatory requirements.

5.2. Risk Mitigation Strategies

5.2.1. Effective risk mitigation requires a multi-layered approach. The following strategies address the specific risk categories identified in this policy.

5.2.2. Market Risk Mitigation

5.2.2.1. Market risk exposure will be regularly assessed, and thresholds for acceptable losses due to volatility will be established. When market risks exceed these thresholds, actions will be taken, such as temporarily halting certain types of transactions or increasing reserve liquidity.

5.2.2.2. The Company will maintain a cryptocurrency reserve with a focus on stable coins and employ hedging strategies (e.g., derivatives or futures contracts) to reduce the financial impact of market volatility on operational funds.

5.2.3. Cybersecurity Risk Mitigation

- 5.2.3.1. The majority of company and player funds will be stored in cold wallets to prevent hacking and cyberattacks. Only operationally necessary funds will be kept in hot wallets.
- 5.2.3.2. Multi-factor authentication will be required for accessing both internal systems and player accounts to reduce the risk of unauthorised access.
- 5.2.3.3. All cryptocurrency transactions and sensitive data will be secured with industry-standard encryption, ensuring confidentiality and integrity.
- 5.2.3.4. Regular external security audits will be conducted to assess system vulnerabilities and ensure that any security gaps are quickly addressed.
- 5.2.3.5. A robust distributed denial-of-service (DDoS) mitigation solution will be implemented to protect the platform from cyberattacks aimed at overwhelming our systems.

5.2.4. Fraud and Financial Crime Risk Mitigation

- 5.2.4.1. Where appropriate, the Company shall implement automated KYC and AML verification systems using blockchain analytics, identity verification tools, and transaction monitoring to detect and prevent fraudulent activity.
- 5.2.4.2. Daily, weekly, and monthly transaction limits will be applied based on risk profiles to prevent money laundering and terrorist financing. Any unusual transaction patterns will trigger alerts for further investigation.
- 5.2.4.3. The Company shall collaborate with leading blockchain analytics and forensic service providers to track the origins and movement of cryptocurrencies across blockchain networks, identifying and blocking tainted funds.
- 5.2.4.4. A designated AML/CFT individuals will be responsible for reviewing Suspicious Transaction Reports (STR) and internal Suspicious Activity Reports (SARs) to further support the efficiency of the escalation process and the reporting to appropriate authorities in compliance with Curacao regulations and, as further highlighted in the Company's AML/CFT Policy.

5.2.5. Operational Risk Mitigation

u

- 5.2.5.1. All cryptocurrency transactions will be automatically monitored for failures or delays, and any issues will trigger immediate alerts for resolution.
- 5.2.5.2. To minimise downtime and ensure operational continuity, the Company will implement redundancy in critical systems, including backup servers, multi-signature wallets, and secondary communication channels.
- 5.2.5.3. A detailed disaster recovery plan will be in place to address potential system failures or security breaches. This plan will include regular data backups, incident response teams, and communication protocols.
- 5.2.5.4. Employees will be trained regularly on annual basis on the latest cryptocurrency related operations and security protocols, ensuring that operational errors and security risks are minimised, including the related risks in AML/CFT areas.

5.2.6. Regulatory Risk Mitigation

- 5.2.6.1. A dedicated compliance team will oversee adherence to Curacao KYC and DD regulations, FATF AML/CFT standards. This team will monitor any regulatory changes and ensure that the Company's policies are updated accordingly. For this purpose, the Company shall also have Compliance Officer appointed.
 - 5.2.6.1.1. The current Nominated Compliance Officer is: Ondrej Zlesak, ondrej.zlesak@yolo.com
- 5.2.6.2. External legal consultants will conduct regular reviews of the Company's legal obligations in different jurisdictions to ensure compliance with tax laws, regulatory filings, and reporting standards.
- 5.2.6.3. To ensure compliance with GDPR, regular data privacy audits will be performed. This includes ensuring proper consent management, data encryption, and secure data transfer procedures.

5.3. Governance and Oversight

5.3.1. Compliance Officer (CO)

- 5.3.1.1. The CO is responsible for overseeing the overall Risk & Compliance strategy and framework. The CO will:

al

- 5.3.1.1.1. develop and maintain Risk & Compliance policies and procedures.
- 5.3.1.1.2. monitor risk exposure, particularly in relation to cryptocurrency.
- 5.3.1.1.3. provide regular updates to the Board of Directors on the effectiveness of risk mitigation strategies.
- 5.3.1.1.4. conduct risk assessments at regular intervals and after significant events (e.g., system upgrades, regulatory changes).
- 5.3.1.1.5. maintain the risk register and update it as new risks are identified, or mitigation strategies evolve.
- 5.3.1.1.6. where necessary, coordinate with external auditors and regulators to ensure compliance with risk management guidelines.

5.3.2. Board of Directors

- 5.3.2.1. The Board of Directors (BoD) has the ultimate responsibility for approving the Company's risk management strategies. BoD will:
 - 5.3.2.1.1. review a regular Compliance & Risk reports submitted by the CO.
 - 5.3.2.1.2. make key decisions on risk tolerance levels and risk appetite.
 - 5.3.2.1.3. provide oversight on significant changes to the Company's risk profile.

5.4. Incident Management and Response

- 5.5. A comprehensive incident response process ensures that when risks materialise, the Company can act swiftly and effectively. The Company will follow a structured response plan set in place in this section.

5.5.1. Incident Response Team (IRT)

N

5.5.1.1. The Incident Response Team will take immediate and appropriate actions in the event of:

5.5.1.1.1. a cybersecurity breach, such as hacking or phishing attempts.

5.5.1.1.2. significant fraud or financial crime event.

5.5.1.1.3. operational system failure affecting the processing of cryptocurrency transactions.

5.5.1.2. The IRT will:

5.5.1.2.1. immediately take necessary steps to contain the threat and assess the impact on the Company and players.

5.5.1.2.2. notify relevant stakeholders, including regulators and affected players, within predefined timeframes.

5.5.1.2.3. perform a root cause analysis and develop a plan to prevent similar incidents in the future.

5.5.2. Escalation Procedures

5.5.3. Incidents are escalated according to severity. Major incidents, such as breaches or regulatory violations, will be escalated to the Board of Directors within 24 hours of discovery and further reviewed by the Compliance Team & CO, providing additional operational support.

5.6. Regular Reviews and Updates

5.6.1. Risk management is a dynamic process, and our strategies must evolve to address new threats and changing regulatory landscapes.

5.6.1.1. The Company will conduct, at minimum, an annual review of the Risk Management Framework to ensure it remains effective and aligned with industry best practices.

5.6.1.2. The Company will also review and update the framework as needed in response to significant changes in the cryptocurrency market, regulatory environment, or technological advancements.

- 5.6.1.3. The Company will incorporate feedback from any and all external auditors, regulators, and stakeholders to continually improve a high level of risk management efforts.

6. Compliance and Reporting

6.1. Internal Reporting:

- 6.1.1. The CO shall submit regular reports on the status changes in cryptocurrency-related risks, mitigation efforts, and compliance with regulations.
- 6.1.2. Any significant risk event (e.g., fraud, cyberattack, or regulatory breach) must be escalated to the Board of Directors within 24 hours.

6.2. Regulatory Reporting:

- 6.2.1. Any suspicious activity involving cryptocurrencies must be reported to Curacao authorities and other relevant bodies in line with our AML/CFT policies.
- 6.2.2. Regular compliance reviews will ensure that risk management efforts remain aligned with regulatory changes and industry best practices.

7. Player Education

- 7.1. To empower players with knowledge about cryptocurrency risks and usage, the following initiatives will be implemented.
 - 7.1.1. Clear language in our T&C sections, explaining the risks of cryptocurrency volatility, fraud, and the importance of secure wallet management.
 - 7.1.2. Regularly updated articles on our site discussing safe cryptocurrency usage, how blockchain technology works, and tips to avoid scams.
 - 7.1.3. Provide 24/7 support through multiple channels (live chat, email) to address any player concerns about cryptocurrency transactions or issues.

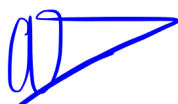
n

8. Ongoing Monitoring

- 8.1. The CO will conduct ongoing monitoring of crypto-related transactions, system vulnerabilities, and new risks (e.g., emerging cryptocurrency technologies).
- 8.2. All crypto transactions are subject to automated monitoring for suspicious activity, including large deposits/withdrawals, irregular betting patterns, and unusual behaviour across accounts.
- 8.3. Use machine learning and AI tools to detect and flag unusual player behaviour for further investigation.
- 8.4. This policy will be reviewed at least annually, or sooner if significant changes in the regulatory or operational environment occur.
- 8.5. This Policy is to be reviewed annually at minimum, or on ad-hoc basis in case of significant events or changes to the areas as captured in this document. the Company's Compliance department is responsible for updating this document together with nominated Compliance Officer.

Document Name: Crypto Risk Assessment Policy v1
Authorized By: eMagnus Curacao B.V./Andrea Engelhardt
Prepared By: Henry Lemendik
Reviewed By: Ondrej Zlesak
Author: mBet Solutions N.V. Compliance Department
Date: October 07, 2024

Signed:



10/7/2024

a