

Crypto Risk Management Policy applicable to Gladiator Holding NV operations

1. Introduction

This Crypto Risk Management Policy ("**Policy**") outlines the procedures, controls, and practices adopted by Gladiator Holding NV ("**the Operator**") to effectively manage the risks associated with cryptocurrency transactions. It is designed to mitigate risks related to money laundering, terrorist financing, fraud, and other financial crimes. The Policy complies with the legal requirements set forth in the Curacao regulatory framework, international anti-money laundering (AML) standards, and the specific needs of the online casino industry.

This Policy applies to all employees, agents, and partners of the Operator and must be adhered to across all gambling activities conducted on the websites operated by the Operator under the Curacao GCB issued license ("**the Website**").

2. Objectives

The primary objectives of the Policy are to:

- Identify and assess the risks associated with cryptocurrency usage.
- Implement controls to mitigate those risks, particularly with respect to AML and Combating the Financing of Terrorism (CFT).
- Establish a framework for ongoing monitoring of cryptocurrency transactions and player behavior.
- Ensure compliance with all relevant legal and regulatory requirements.

3. Risk Categories and Assessment

The Operator shall categorize and assess the risks associated with cryptocurrency transactions by analyzing the following risk factors:

3.1. Player Jurisdiction Risk

Certain jurisdictions pose a higher risk of money laundering and financial crime. The Operator will maintain an updated list of high-risk jurisdictions based on FATF recommendations and local Curacao guidance.

- **High-Risk Jurisdictions:** Players residing or operating from high-risk jurisdictions must undergo enhanced due diligence (EDD) before being allowed to transact in cryptocurrencies.
- **Prohibited Jurisdictions:** The Website will block access to players from jurisdictions that are blacklisted or prohibited under Curacao law.

3.2. Player Status Risk

Players with certain profiles may present higher risks, requiring additional scrutiny:

- **Politically Exposed Persons (PEPs):** Any player identified as a PEP must undergo enhanced due diligence. The Operator will identify PEPs through the KYC process and ensure additional verification measures are in place.
- **Sanctioned Individuals or Entities:** The Operator will ensure that any player listed in global or national sanction databases is prohibited from accessing the Website.

3.3. Transaction Risk

Cryptocurrency transactions, due to their anonymity and speed, present additional risks:

- **Large Transactions:** Any cryptocurrency deposit or withdrawal exceeding a specified threshold (set by the Operator) will trigger extended KYC procedures and source-of-funds verification.
- **Suspicious Transactions:** The Operator will monitor for transactions that are unusual based on the player's profile or gaming behavior (e.g., rapid and large deposits or withdrawals, or transactions using multiple wallets). Suspicious transactions will be reported to relevant authorities and may trigger further internal investigation.

3.4. Cryptocurrency Type Risk

Each cryptocurrency has unique risk characteristics that must be considered:

- **Bitcoin (BTC) and Ethereum (ETH):** Both are considered widely used cryptocurrencies, but due to their popularity and liquidity, they may also be more attractive for illicit activities. Transactions in BTC and ETH must be closely monitored for red flags.
- **USDC:** Stablecoins like USDC are tied to fiat currency and may present different money laundering risks, particularly involving cross-border transactions.
- **Bitcoin Cash (BCH):** BCH is less widely used but still poses risks of anonymity and decentralized transactions.

4. Cryptocurrency Transaction Risk Management Procedures

4.1. Onboarding and KYC Procedures

- **Basic KYC:** All players must complete identity verification before being allowed to deposit cryptocurrency on the Website. The verification process includes:
 - Submission of a valid government-issued ID.
 - Proof of address (utility bill, bank statement, etc.).
 - Date of birth verification to ensure legal age.
- **Enhanced KYC:** Prior to any withdrawal or large cryptocurrency transaction, the Operator must perform enhanced KYC. This includes verifying the source of funds and ensuring the player's account is not linked to any suspicious activities or red flags.

4.2. Cryptocurrency Wallet Verification

Players must provide a registered cryptocurrency wallet before making any deposits or withdrawals. The Operator will:

- Verify the ownership of the cryptocurrency wallet.
- Monitor wallet addresses for any link to illegal activities using third-party blockchain analytics tools.
- Ensure wallets involved in high-risk jurisdictions or linked to suspicious activity are flagged for additional scrutiny.

4.3. Transaction Monitoring

The Operator will deploy robust monitoring systems for real-time analysis of cryptocurrency transactions on the Website. These systems will:

- Track deposits, withdrawals, and in-game transactions.
- Identify suspicious patterns such as large, frequent, or irregular transactions.
- Flag and hold transactions until further verification if necessary.

5. Ongoing Monitoring and Reporting

5.1. Ongoing Player Monitoring

After the initial onboarding, the Operator must maintain a continuous monitoring system to detect changes in player risk profiles:

- **Behavioral Monitoring:** Monitor gaming patterns and betting activity to identify any unusual behavior.
- **Risk Profile Updates:** Players initially classified as low or medium risk may be reassessed as high risk if their activities or background information change (e.g., becoming a PEP).

5.2. Automated Transaction Monitoring Tools

- The Operator will use blockchain analytics tools to assess the origin of cryptocurrency funds and trace suspicious wallet activity.
- Transaction alerts will be generated based on predefined parameters, such as transfers to or from high-risk jurisdictions, unusual transaction amounts, or frequent transfers between multiple wallets.

5.3. Suspicious Activity Reporting (SAR)

The Operator is required to report suspicious activities to the relevant authorities in Curacao, in accordance with the local AML/CFT legislation:

- All suspicious or unusual transactions must be logged and reported within the legally mandated time frame.
- Employees and staff must be trained to identify and escalate potential red flags to the Operator's AML Compliance Officer.

6. Training and Awareness

All employees and agents involved in handling cryptocurrency transactions and player activities must receive comprehensive training on:

- AML and CFT obligations.
- Recognizing red flags associated with cryptocurrency transactions.
- Using blockchain monitoring tools and identifying suspicious wallet activity.
- Understanding the risks associated with specific jurisdictions and player profiles.

Regular refresher courses will be conducted to keep employees updated on the evolving regulatory environment and emerging risks in cryptocurrency usage.

7. Record-Keeping and Data Security

The Operator will maintain detailed records of:

- Player identities, verification documents, and ongoing monitoring notes.
- Cryptocurrency transactions, including deposits, withdrawals, and in-game transfers.
- Any reports submitted to relevant authorities, including SARs.

All data must be stored securely and in compliance with data protection regulations to prevent unauthorized access or tampering.

8. Compliance Reviews and Policy Updates

- The Operator will conduct periodic internal audits and compliance reviews to ensure that all aspects of the Crypto Risk Management Policy are followed effectively.
- The Policy will be reviewed and updated annually or as required by changes in legal, regulatory, or operational requirements.

9. Conclusion

This Crypto Risk Management Policy ensures that the Operator adheres to best practices in the management of cryptocurrency-related risks. By focusing on proper onboarding, transaction monitoring, and ongoing due diligence, the Operator minimizes the risk of money laundering, fraud, and other illicit activities on the Website.

All employees, partners, and agents are responsible for implementing this Policy and ensuring compliance with its provisions at all times.