

Draft Risk Assessment Policy Statement for an Online Casino

1. Introduction

This Risk Assessment Policy Statement ("Policy") outlines the comprehensive procedures Zaptorica B.V. ("Company") will undertake to identify, assess, mitigate, and report on the risks associated with Money Laundering (ML) and Terrorist Financing (TF) in accordance with the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regulations set forth by the Curaçao Gaming Control Board (GCB). The Company recognizes the importance of maintaining a safe and secure online casino environment that is free from criminal activity. We are committed to upholding the highest standards of financial integrity and preventing our platform from being used for illegal purposes.

2. Risk Assessment Framework

The Company will maintain a comprehensive and ongoing risk assessment framework to effectively identify, analyze, and prioritize potential ML/TF risks. This framework will be based on a risk-based approach, considering various factors such as:

- **Customer Risk Assessment:**
 - **Geography:** We will analyze the risk profiles of customer locations based on known ML/TF vulnerabilities in specific regions.
 - **Source of Funds:** We will implement robust Customer Due Diligence (CDD) procedures to verify the legitimacy of customer funds and identify potential high-risk sources.
 - **Transaction Activity:** We will monitor customer transaction patterns for anomalies, focusing on large or frequent transactions, unusual geographic destinations of funds, or activity inconsistent with declared income levels.
- **Product and Service Risk Assessment:**
 - **Game Types:** We will assess the inherent ML/TF risks associated with different casino games, prioritizing those with higher potential for anonymity or rapid movement of funds (e.g., high-roller tables, anonymous betting options).
 - **Payment Methods:** We will evaluate the ML/TF risks associated with various payment methods, such as cryptocurrencies and lesser-known

payment processors, implementing enhanced due diligence for high-risk methods.

- **Bonus Structures:** We will analyze the potential for bonus misuse in ML/TF schemes, implementing appropriate limitations and monitoring for bonus abuse patterns.
- **Delivery Channel Risk Assessment:**
 - **Online Platform:** We will maintain robust security measures on our online platform to prevent unauthorized access, data manipulation, and account takeovers.
 - **Mobile Applications:** We will apply the same security standards to our mobile applications, focusing on secure logins, transaction encryption, and device verification.
 - **Third-Party Integrations:** We will conduct thorough due diligence on all third-party vendors and partners integrated with our platform, ensuring they adhere to strong AML/CFT practices.

3. Risk Mitigation Strategies

Based on the risk assessment framework, the Company will implement a multi-layered approach to mitigate ML/TF risks:

- **Customer Due Diligence (CDD):**
 - **Know Your Customer (KYC):** We will implement stringent KYC procedures to verify customer identities, including document verification, address confirmation and ongoing monitoring of customer information.
 - **Enhanced Due Diligence (EDD):** We will apply Enhanced Due Diligence for high-risk customers based on the risk assessment, requiring additional information and source of funds verification.
 - **Continuous Monitoring:** We will maintain ongoing customer monitoring to identify any changes in risk profiles or suspicious activity that may require further investigation.
- **Suspicious Activity Monitoring (SAM):**
 - **Transaction Monitoring:** We will implement a robust transaction monitoring system to identify suspicious transactions based on pre-defined rules and red flags.
 - **Case Management:** We will establish a system for investigating and escalating suspicious activity reports (SARs) to the designated AML Compliance Officer.

- **Scenario Testing:** We will regularly conduct scenario testing to identify and address emerging ML/TF typologies and update our detection mechanisms accordingly.
- **Reporting:**
 - **Internal Reporting:** We will maintain clear reporting procedures for SARs submitted to the AML Compliance Officer, ensuring timely escalation to management and regulatory authorities.
 - **External Reporting:** We will comply with all regulatory reporting requirements mandated by the GCB, including timely submission of SARs and other relevant AML/CFT reports.
- **Employee Training:**
 - **Regular Training:** We will provide ongoing training to all employees on AML/CFT regulations, identification of suspicious activity, and reporting procedures.
 - **Role-Specific Training:** We will conduct role-specific training for employees with high AML/CFT risk exposure, such as customer support and transactions teams.

4. Management Oversight and Review

The Company's AML/CFT program will be overseen by a designated AML Compliance Officer who is responsible for implementing and maintaining the program, reporting to senior management, and ensuring adherence to regulatory requirements. The Risk Assessment Policy will be reviewed and updated periodically, or as needed, to reflect any changes in the business environment, regulatory landscape,

Specific action plan as undertaken per risk Category:

Customer Risk Assessment:

- **Geography:** We will analyze the risk profiles of customer locations based on known ML/TF vulnerabilities in specific regions. **Action:** Maintain a continuously updated list of high-risk jurisdictions based on GCB and international AML/CFT watchlists.
- **Source of Funds:** We will implement robust Customer Due Diligence (CDD) procedures to verify the legitimacy of customer funds and identify potential high-risk sources. **Action:** Require customers to provide detailed documentation and explanations for large deposits or funds from high-risk sources.

- **Transaction Activity:** We will monitor customer transaction patterns for anomalies, focusing on large or frequent transactions, unusual geographic destinations of funds, or activity inconsistent with declared income levels. **Action:** Implement transaction monitoring software with pre-defined rules to flag suspicious activity, such as exceeding transaction limits or rapid accumulation of winnings.
- **Product and Service Risk Assessment:**
 - **Game Types:** We will assess the inherent ML/TF risks associated with different casino games, prioritizing those with higher potential for anonymity or rapid movement of funds (e.g., high-roller tables, anonymous betting options). **Action:** Implement stricter verification and transaction limits for high-risk games, and consider additional monitoring for suspicious betting patterns.
 - **Payment Methods:** We will evaluate the ML/TF risks associated with various payment methods, such as cryptocurrencies and lesser-known payment processors, implementing enhanced due diligence for high-risk methods. **Action:** Prohibit anonymous payment methods or require additional verification for high-risk payment processors.
 - **Bonus Structures:** We will analyze the potential for bonus misuse in ML/TF schemes, implementing appropriate limitations and monitoring for bonus abuse patterns. **Action:** Set clear bonus wagering requirements, limit the frequency of bonus redemptions, and monitor for suspicious bonus claiming patterns across multiple accounts.
- **Delivery Channel Risk Assessment:**
 - **Online Platform:** We will maintain robust security measures on our online platform to prevent unauthorized access, data manipulation, and account takeovers. **Action:** Implement multi-factor authentication for logins, encrypt all customer data, and conduct regular security audits of the platform.
 - **Mobile Applications:** We will apply the same security standards to our mobile applications, focusing on secure logins, transaction encryption, and device verification. **Action:** Require strong passwords and biometric authentication (where applicable) for mobile app logins, encrypt all transactions within the app, and implement device verification procedures.
 - **Third-Party Integrations:** We will conduct thorough due diligence on all third-party vendors and partners integrated with our platform, ensuring they adhere to strong AML/CFT practices. **Action:** Include contractual

clauses requiring third-party partners to comply with AML/CFT regulations and conduct periodic reviews of their AML compliance programs.

3. Risk Mitigation Strategies

Based on the risk assessment framework, the Company will implement a multi-layered approach to mitigate ML/TF risks:

- **Customer Due Diligence (CDD):**
 - **Know Your Customer (KYC):** We will implement stringent KYC procedures to verify customer identities, including document verification, address confirmation and ongoing monitoring of customer information. **Action:** Require high-quality scans of government-issued IDs, conduct address verification checks, and request proof of income for high-risk customers.
 - **Enhanced Due Diligence (EDD):** We will apply Enhanced Due Diligence for high-risk customers based on the risk assessment, requiring additional information and source of funds verification. **Action:** Collect information on the purpose and intended use of funds on the platform, and obtain written explanations for suspicious transactions.
 - **Continuous Monitoring:** We will maintain ongoing customer monitoring to identify any changes in risk profiles or suspicious activity that may require further investigation. **Action:** Conduct periodic reviews of customer activity, update customer information as needed, and trigger alerts for significant changes in transaction patterns or account behavior.