1. Anti money laundering policy;

As part of our commitment to conducting business ethically and maintaining the highest standards of integrity, MERVCF Limited has adopted a zero-tolerance policy on money laundering. Money laundering is a serious crime that can damage the integrity of our business and have harmful consequences for society as a whole.

Measures to prevent money laundering

1. **Identification and verification of participants**: We will operate a robust system for identifying and verifying participants in our lottery, requiring relevant IDs and documentation to verify the validity of their participation.
2. **Transaction Monitoring:** We will carefully monitor and analyze all transactions that occur within our lottery to identify suspicious activity, such as unusual large transactions, frequent transactions to and from various wallet accounts, or patterns that deviate from normal behavior.
3. **Education and awareness:** We will provide our staff with training and resources to make them aware of the risks of money laundering and help them recognize and report suspicious activity.
4. **Cooperation with Law Enforcement Agencies:** We will work closely with relevant law enforcement agencies and government organizations to investigate and report suspicious activity, and to comply with all legal requirements related to the prevention of money laundering.
5. **Periodic Review and Review:** We will regularly review and revise our policies and procedures as necessary to ensure that they remain effective in preventing money laundering in our lottery.
6. **Each player can buy a maximum of 100 tickets in each lottery.**

2. Company Policy Statement

MervCF Limited is not a financial institution within the meaning of applicable law of Costa Rica and is accordingly not directly subject to the statutes and regulations applicable to certain financial institutions, money transfer, or virtual asset service providers. However, in accordance with the 2016 Regulations for Anti-Money Laundering and Combating the Financing of Terrorism ("AML/CFT") applicable for the Costa Rica jurisdiction, MervCF Limited11 expressly prohibits and rejects the use of MervCF Limited products for any form of illicit activity, including money laundering, terrorist financing or trade sanctions violations, consistent with various national anti-money laundering ("AML") laws, regulations and norms. MervCF Limited continues to monitor norm setting parameters promulgated by the Financial Action Task Force ("FATF") and certain gaming trade groups in addition to the Costa Rica Gaming Control Board and will take necessary action as it deems appropriate to reflect changes in law.

MervCF Limited's intention is to follow global best practices in guarding against MervCF Limited products being used to facilitate such activities. Those best practices include:

- Adoption of a written policy, and procedures and controls, reasonably designed to guard against money laundering, terrorist financing and trade sanctions violations;
- Where appropriate, designation of a compliance officer to oversee the implementation of the policy, procedures and controls;
- Provision of related education and training to relevant personnel; and
- Independent reviews, monitoring and maintenance of the policy, procedures and controls.

3. Definitions

The following defined terms are widely used in the industry:

Money Laundering: The process of making illegally-gained proceeds appear legal. This process is generally broken down into three steps: placement, layering and integration.

Placement: The process of placing unlawful proceeds into traditional financial institutions, through deposits or other avenues.

Layering: The process of separating proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler's checks, money orders, wire transfers, letters of credit, stocks, bonds or purchasing assets.

Integration: Using apparently legitimate transactions to disguise the illicit proceeds, allowing the laundered funds to be distributed back to the criminal; integrating the now clean money back into normal use.

Suspicious Activity: Activity conducted by a user or non-user using the institution where there are indications that the persons engaging in the transaction may be doing so for fraudulent or illegal purposes.

Sanctions: Sanctions are activities conducted by the international community to prohibit or constrain activities of the target of the sanctions.For example, they are used:

- To encourage a change in behaviour for a target country or regime;
- To apply pressure on a target country to comply with set objectives;
- As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed; or
- To prevent and suppress the financing of terrorists or terrorist acts.

4. Governance and Oversight

MervCF Limited has appointed a Chief Compliance Officer ("CCO") that is responsible for coordinating the implementation of the AML Policy and policy program. The Chief Compliance Officer's duties also include developing AML initiatives, work with other MervCF Limitedholders to revising the AML policy, assessing new regulatory requirements and investigate potentially suspicious or unusual activity. MervCF Limited also provides AML training to all of its employees on a regular basis.

5. Know Your Customer and Transaction Monitoring

MervCF Limited will apply appropriate user due diligence and ongoing monitoring measures required by law. MervCF Limited will endeavour to prevent users from engaging in illicit or otherwise unauthorised activity. MervCF Limited uses a combination of its software development and other service agreements, which are enforced through internal operational features to ensure that it complies with the applicable law.

Know Your Customer

A. Customer Due Diligence.

MervCF Limited has adopted a risk based CDD to enable MervCF Limited to understand the nature and purpose of the user relationship to the MervCF Limited platform in order to develop a customer risk profile. In order to do so, MervCF Limited collects certain documentary and non-documentary information at account-opening commensurate with the nature of the type account and services that MervCF Limited offers. MervCF Limited maintains different CDD for different accounts and services.

For instance, the CDD requires users go through MervCF Limited's customer identification program ("CIP"). The CIP consists of procedures for:

- Collecting baseline (e.g., wallet address, email address) information at account creation through MervCF Limited's user onboarding portal;
- Monitoring the risk profile associated with the underlying cryptocurrency wallet used to fund the user's account;
- Maintaining records of the information used to identify the user; and
- Determining if a user appears on any list of known or suspected terrorists or terrorist organisations provided to the financial institutions based on the above information.

The above steps are operationalised using the following measures:

- *Identity and Age Verification*. A third-party service provider will support's MervCF Limited's ability to determine the legitimacy of the identification information other KYC materials or information provided and will confirm that the user is permissible. The service provider also will confirm that the user does not appear to be located in a comprehensively-sanctioned or otherwise prohibited jurisdiction and will search global sanctions lists to confirm that the user does not appear thereon using onboarding information such as wallet addresses.
- *Customer Information*. MervCF Limited will collect details on each user to form a reasonable belief that MervCF Limited knows the identity of its users commensurate with the user's risk profile. For instance, MervCF Limited may collect such details as the wallet address, name, address, country, date of birth, or postal code (collectively, "KYC Information"). MervCF Limited will collect any of the above KYC Information prior to issuing a MervCF Limited funding address (e.g., QR code) to users. MervCF Limited does not presently allow users who are non-natural persons.MervCF Limited may, at its own description rely on the performance by another institution of some or all of the elements of our CIP.

- *Geo-blocking for Prohibited Jurisdictions*. MervCF Limited will require contractual client certifications that, through IP address-based geo-blocking, no gaming services will be offered in countries where such activity is not permitted.
- *Geo-blocking for Sanctioned Jurisdictions*. MervCF Limited also will require contractual client certifications that such users are not subject to United States, European Union, or other global sanctions or watch lists, including individuals or entities associated with the United States' comprehensively sanctioned jurisdictions, Iran, Cuba, North Korea, Syria and the Crimean region of Ukraine. MervCF Limited will rely on various risk-based measures to verify these representations including as in the below-described know-your-user ("KYC") measures and through IP address-based geo-blocking.
- *Contractual Prohibitions on Users Onboarding from Prohibited Jurisdictions*. Users are notified at onboarding that MervCF Limited does not offer services in restricted jurisdictions. MervCF Limited's policy on restricting user activity stems from a combination of its risk, fraud prevention, and AML standards, as well as any assessments associated with the permissibility of its services in certain jurisdictions.

B. Enhanced Due Diligence and Ongoing Monitoring

MervCF Limited performs ongoing monitoring on its users in order to detect any behaviours or indicators that might raise suspicions in regard to money laundering and terrorism financing practices. For that purpose, MervCF Limited has implemented a set of red flag indicators that help it determine such behaviours and require further action from MervCF Limited in assessing the customer information.

Whenever one of those red flags is triggered, the user account will be suspended and MervCF Limited will pursue enhanced due diligence. Enhanced KYC diligence under this policy is deemed to include, but not limit to, the provision of:

- Full legal name;
- Country of citizenship;
- Permanent Address (which, for an individual, must be a residential or business street address, and for an entity, must be a principal place of business, local office or other physical location);
- Identification number (either a taxpayer identification number, or, if unavailable, a passport number and country of issuance, alien identification card number or number and country of issuance of another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard);
- Identification Document; and
- Source of Funds and Source of Wealth.

MervCF Limited may use third party service provider to verify any of the above information as determined to establish a reasonable basis to know the true identity of the user where the user's activity warrants such action.

C. Acceptance Policy

MervCF Limited will not accept a and will block the users that:

- Do not provide the identification information requested by MervCF Limited;
- Provide fake identification documents;
- Try to use different means to deceive about their location;
- Are from restricted or prohibited jurisdictions; or
- Are subjected to United States, European Union, or other global sanctions or watch lists;
- Are gambling addicted or have mental health issues;
- Its source of funds are originated or exchanges in restricted jurisdictions;

MervCF Limited reserves the right to block and suspend player for any other reasons at its own description

Transactions Monitoring

MervCF Limited is firmly committed to complying with economic and trade sanctions programs imposed by jurisdictions in which the firm conducts business. For that purpose MervCF Limited established a transaction monitoring program with controls and processes to identify and detect any unusual activity in real time and in its ongoing monitoring.

MervCF Limited will conduct ongoing monitoring on a regular basis using rule-based systems developed in-house and others from third-party vendors to review user history and patterns of activity to detect and report any unusual activity as required and to develop and implement any additional controls or limits in its platform.

MervCF Limited implemented procedures addressing the following two key components of unusual or suspicious activity management:

- identification of unusual activity through methods of identification may include employee and customer identification, law enforcement inquiries, other referrals, or transaction and surveillance monitoring system reports; and
- alert management that focuses on processes used to investigate, evaluate and document identified unusual or potentially suspicious activity.

MervCF Limited will use the following processes to achieve both goals:

- *Transaction Monitoring for Sanctioned or Prohibited Jurisdictions*. MervCF Limited may in its reasonable discretion impose certain due diligence requests at user balance withdrawal. MervCF Limited presently conducts a mixture of manual and automated transaction monitoring processes to identify “red flag” behaviour. Where such red flag behaviour is identified, MervCF Limited may refuse to process any withdrawal attempts or collect additional information from the recipient. MervCF Limited will further endeavour to limit any attempted user account funding from prohibited jurisdictions (which are identified in the MervCF Limited user facing disclosures and updated from time to time internally) where the associated wallet address indicates that the user or the user’s funds are located in such a prohibited jurisdiction. For instance, MervCF Limited may prohibit a user from funding their MervCF Limited account using a known U.S. based exchange wallet as such assets

indicate that the user is a U.S. person. Users will have the ability to rebut any suspension with additional information as part of MervCF Limited's ongoing transaction monitoring and user due diligence standards.

- *Screening for Sanctioned Parties.* Prior to issuing a MervCF Limited funding address to a user, MervCF Limited will screen a user's wallet address against applicable sanctions databases. Such screening measures will rely on third party blockchain forensics vendors such as Chainalysis. MervCF Limited will periodically re-screen wallet addresses against such databases.
- *Identification of Unusual Activity*. MervCF Limited will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to its business. Monitoring will be conducted running regular reports of unusual, high risk, or suspicious user activity.
- *Anti-Mixing Measures.*MervCF Limited will utilise software designed to detect other suspicious deposit or withdrawal patterns. Such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk. In such instances, a user may be required to explain their methodology and purpose for using the platform.
- *Chainalysis Review.* Every single crypto deposit or withdrawal both indirect and direct will run through Chainalysis and reviewed for signs of fraud or suspicious behaviour. A user's account will be suspended and reviewed upon alert of potential illicit behaviour. Sufficient proof of wealth may be requested from high-risk accounts. MervCF Limited may refuse to withdraw to certain "high-risk" addresses as determined in consultation with Chainalysis risk scoring.
- *Withdrawal Threshold KYC.* Additionally, and independently, every account, wherever or with whomever associated, will be suspended until adequate KYC diligence occurs once that account reaches a withdrawal threshold dependent on the accounts risk characterisation over the life of the account.

D. Other Ongoing Monitoring Controls

Additionally to the above mentioned controlling procedures, MervCF Limited has also implemented the following procedures to complement its know your customer and ongoing monitoring procedures:

- *Ban Evasion Detection*. In addition, MervCF Limited will utilise third-party service provider software designed to detect the use by one user of multiple accounts. This software relies on detection of links between the same devices used to access multiple accounts. Such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk. In such instances, a user may be required to explain their methodology and purpose for using the platform. MervCF Limited accounts are funded by users using local (non-custodial) or hosted (custodial) wallets. In addition to a Chainalysis screening, MervCF Limited monitors user activity within the MervCF Limited platform and any withdrawals must meet MervCF Limited's and its third-party service provider's verification processes. MervCF Limited further prohibits peer-to-peer account transfers within the MervCF Limited platform infrastructure. Any attempts to circumvent this restriction will be treated as a red flag.

- *Time Zone Monitoring.* MervCF Limited has implemented time zone controls that detects the users device information and crosses it with restricted jurisdiction to understand if they are trying to use geo location software to hide the jurisdictions where they are connecting from.
- *Products and Services Review.* MervCF Limited will establish additional procedures to avoid facilitating user attempts to exploit the MervCF Limited platform. MervCF Limited has a robust set of user-facing terms that users attest to in order to utilise the MervCF Limited platform. MervCF Limited will establish certain additional safeguards to mitigate against the risk of such misuse. For instance, MervCF Limited may establish policies or procedures for limiting which user assets can be onboarded to the MervCF Limited platform. MervCF Limited lists the assets that are available for use on the MervCF Limited platform. MervCF Limited does not allow the use of anonymity enhancing technologies such as mixers, tumblers, or certain coins and tokens. Where MervCF Limited becomes aware that an anonymity enhancing technology is being used on the MervCF Limited platform, MervCF Limited will disallow such use.
- *Vendor Management.* MervCF Limited works with reputable third-party service providers as part of its compliance infrastructure. MervCF Limited will periodically assess the strength of its key third party service providers to determine if additional services are needed, the third-party service provider is not performing consistent with its contractual obligations, or if other remedial action is necessary for MervCF Limited to comply with this policy. MervCF Limited may request information from any third-party service provider as part of its vendor review process.
- *Compliance Innovation*. In addition to vendor management, MervCF Limited will continuously monitor any non documentary compliance mechanisms to determine their viability for the MervCF Limited program. MervCF Limited may run test or trial programs on a limited basis with such compliance vendors to determine the effectiveness of such programs. Blockchain native compliance tools include fraud prevention services, on-chain KYC providers, and other tools designed to reflect the technological features associated with blockchain platforms.

6. Education and Training

MervCF Limited, with the assistance of its legal counsel and under the oversight of its CCO, may provide employees AML, anti-terrorist financing and trade sanctions compliance training on a periodic basis, as deemed appropriate.

7. Reporting

MervCF Limited is obliged to report any unusual or suspicious transactions, in accordance with the National Ordinance. Customers that are identified as being on a sanctions list, linked to money laundering or terrorism financing or other criminal activities will be reported as suspicious activity to the regulator