

CRYPTO POLICY

K.I.K. Corporation B.V.

232Casino

Version 1.0

Effective Date: 10/07/2026

Approved by: Board of Directors

Approved by: Compliance Officer

1. Purpose

The purpose of this Crypto Policy is to establish the principles, controls and procedures governing the acceptance, processing, monitoring and management of cryptocurrency transactions conducted through **232Casino**, operated by **K.I.K. Corporation B.V.**, in accordance with the requirements of the Curaçao Gaming Authority (CGA).

This Policy establishes the framework for the secure and compliant use of virtual assets within the licensed gaming operation and aims to ensure:

- compliance with the National Ordinance on Games of Chance (LOK), the applicable CGA Policy Guidelines, AML/CFT legislation and other relevant regulatory requirements;
- protection of the integrity of the Company's gaming operations;
- effective management of money laundering, terrorist financing, fraud, sanctions and other financial crime risks associated with virtual assets;
- implementation of appropriate governance, transaction monitoring and reporting procedures for cryptocurrency transactions;
- protection of players and company assets through appropriate operational and security controls.

This Policy complements the Company's existing AML/CFT Policy, Business Risk Assessment, Enhanced Due Diligence Procedure, Transaction Monitoring Procedures, Incident Reporting Procedure and other internal compliance documents. Where cryptocurrency transactions are involved, the requirements of this Policy shall apply in addition to all other applicable internal policies and regulatory obligations.

2. Scope

This Crypto Policy applies to the licensed online gaming operations of **K.I.K. Corporation B.V.**, operating under the **232Casino** brand.

The Policy governs the acceptance, processing, monitoring and management of cryptocurrency transactions relating to player deposits, wagering activities, withdrawals and any associated operational processes conducted under the Company's Curaçao gaming licence.

This Policy applies to all directors, officers, employees and relevant third-party service providers involved in the processing, monitoring or oversight of cryptocurrency transactions within the licensed operation.

The Company currently accepts cryptocurrency payments exclusively for **232Casino**. The **AllTheBestLottos** brand does not currently offer cryptocurrency payment methods and therefore falls outside the scope of this Policy.

Cryptocurrency payment processing is facilitated through the Company's appointed payment arrangements. The Company currently utilises **CoinsPaid** services through **Dream Finance Processing Inc.**, acting as the payment provider under the contractual arrangements concluded with **Holzman Limited**, an affiliated group company providing payment support services to the licensed operation. Notwithstanding these arrangements, **K.I.K. Corporation B.V.** remains fully responsible for compliance with all applicable regulatory, AML/CFT and licensing obligations relating to cryptocurrency transactions conducted under its Curaçao gaming licence.

This Policy applies to all supported cryptocurrencies made available by the Company through its approved payment provider(s) and shall be read together with the Company's AML/CFT Policy, Business Risk Assessment, Enhanced Due Diligence Procedure, Transaction Monitoring Procedures, Incident Reporting Procedure and any other applicable internal compliance policies.

3. Definitions

For the purposes of this Policy, the following definitions shall apply:

Virtual Asset (VA)

A digital representation of value that can be digitally traded, transferred or used for payment or investment purposes, including cryptocurrencies accepted by the Company for licensed gaming activities.

Virtual Asset Service Provider (VASP)

A legal entity providing virtual asset-related services, including the exchange, transfer, custody or administration of virtual assets on behalf of customers. For the purposes of this Policy, the Company utilises approved third-party providers for crypto payment processing and does not itself operate as a VASP.

Blockchain Analytics

The process of analysing blockchain transactions and wallet activity using specialised tools and services to identify transaction origins, destinations, sanctions exposure, suspicious activity and other financial crime risks.

Wallet Ownership Verification

The process of verifying that a customer owns or controls a cryptocurrency wallet

before withdrawals are processed or where enhanced verification is considered necessary.

Hosted Wallet

A cryptocurrency wallet managed by a regulated Virtual Asset Service Provider on behalf of the customer.

Unhosted (Self-Hosted) Wallet

A cryptocurrency wallet controlled directly by the customer without the involvement of a Virtual Asset Service Provider.

Travel Rule

The international standard established under FATF Recommendation 16 requiring certain originator and beneficiary information to accompany virtual asset transfers between regulated Virtual Asset Service Providers, where applicable.

Enhanced Due Diligence (EDD)

Additional customer due diligence measures applied to higher-risk customers or transactions in accordance with the Company's AML/CFT Policy and Enhanced Due Diligence Procedure.

Sanctioned Wallet

A cryptocurrency wallet identified as being subject to applicable international sanctions or otherwise prohibited under applicable legislation or recognised blockchain analytics providers.

Privacy-Enhancing Cryptocurrency

A cryptocurrency designed to obscure transaction details or wallet ownership, thereby limiting effective blockchain monitoring and source-of-funds verification.

Approved Crypto Assets

Cryptocurrencies formally approved by the Company following documented risk assessment and made available through the Company's authorised crypto payment provider(s).

4. Regulatory Framework

This Policy has been developed in accordance with the applicable legal and regulatory requirements governing the use of cryptocurrencies in licensed online gaming operations in Curaçao. It should be read in conjunction with the Company's internal compliance framework and all other applicable laws, regulations and regulatory guidance.

The Company shall ensure that this Policy is reviewed and updated whenever there are material legislative, regulatory or operational changes affecting cryptocurrency activities.

The primary regulatory framework applicable to this Policy includes, but is not limited to, the following:

Regulation / Standard	Purpose
National Ordinance on Games of Chance (LOK)	Establishes the legal framework governing the licensing and supervision of online gaming operators in Curaçao.
CGA Crypto Policy Guideline (June 2026)	Sets out the regulatory expectations for the acceptance, processing, monitoring and management of cryptocurrency transactions by licensed online gaming operators.
CGA AML/CFT Policy and related AML Guidelines	Establishes AML/CFT obligations applicable to both fiat and cryptocurrency transactions.
National Ordinance on the Reporting of Unusual Transactions (NORUT)	Establishes the legal obligations relating to the identification and reporting of unusual transactions to the Financial Intelligence Unit (FIU).
National Ordinance on Identification when Rendering Services (NOIS)	Establishes customer identification and verification requirements.
Sanctions National Ordinance and applicable international sanctions regimes	Requires screening against applicable sanctions lists and prohibits transactions involving sanctioned persons, wallets or entities.
FATF Recommendations	Provides internationally recognised standards for AML/CFT, including Recommendation 15 (Virtual Assets and VASPs) and Recommendation 16 (Travel Rule).

In addition to the above regulatory framework, this Policy operates together with the Company's internal governance and compliance documentation, including but not limited to:

- AML/CFT Policy;
- Business Risk Assessment;
- Customer Risk Assessment Methodology;
- Enhanced Due Diligence (EDD) Procedure;
- Transaction Monitoring Procedures;
- Incident Reporting Procedure;
- Operations Manual;
- Information Security Policy;
- Any other policies and procedures governing payments, fraud prevention, responsible gaming, record retention and regulatory compliance.

Where any conflict arises between this Policy and applicable legislation or mandatory regulatory requirements, the applicable law or regulatory requirement shall prevail.

5. Governance and Responsibilities

5.1 Governance

The Company is committed to maintaining effective governance over all cryptocurrency-related activities conducted under its Curaçao gaming licence.

The Board of Directors retains ultimate responsibility for ensuring that cryptocurrency activities are conducted in a safe, transparent and compliant manner and that appropriate governance, risk management and internal control measures are maintained.

This Policy shall be approved by the Board of Directors and signed by the Compliance Officer prior to its implementation. It shall be reviewed at least annually or earlier where required due to regulatory, operational or business changes.

Any material amendment to this Policy, including the addition or removal of supported crypto assets, payment providers, wallet arrangements or significant risk controls, shall be subject to documented review and approval.

5.2 Roles and Responsibilities

Board of Directors

The Board of Directors is responsible for:

- approving this Crypto Policy and any subsequent material amendments;
- overseeing the Company's cryptocurrency risk management framework;
- ensuring sufficient resources are allocated for compliance with applicable regulatory requirements;
- promoting an effective compliance culture throughout the organisation.

Compliance Officer

The Compliance Officer is responsible for:

- overseeing compliance with this Policy and all applicable AML/CFT obligations;
- monitoring regulatory developments relating to cryptocurrency activities;
- ensuring that appropriate customer due diligence, Enhanced Due Diligence (EDD), sanctions screening and transaction monitoring controls are maintained;
- reviewing and escalating suspicious or unusual cryptocurrency activity where appropriate;
- coordinating regulatory reporting where legally required;
- ensuring that relevant personnel receive appropriate compliance training.

Finance Department

The Finance function is responsible for:

- maintaining accurate accounting records relating to cryptocurrency transactions;
- performing reconciliations of cryptocurrency-related financial activity where applicable;
- supporting financial reporting and audit requirements;
- cooperating with Compliance in the investigation of unusual transactions.

Operations and Payments

Personnel responsible for payment operations shall:

- oversee the operational processing of cryptocurrency deposits and withdrawals;
- ensure transactions are processed only through approved payment providers;
- apply operational controls relating to payment processing and customer verification;
- immediately escalate any irregular or suspicious activity to the Compliance Officer.

Information Technology

The Information Technology function is responsible for:

- maintaining secure integration with approved cryptocurrency payment providers;
- protecting systems used for cryptocurrency payment processing;
- implementing appropriate access controls, authentication measures and cybersecurity safeguards;
- supporting transaction monitoring, system logging and incident investigations where required.

Employees

All employees involved in cryptocurrency-related activities are responsible for:

- complying with this Policy and all related internal procedures;
- promptly reporting suspicious, unusual or potentially fraudulent activity;
- participating in mandatory compliance and AML/CFT training;
- protecting confidential customer and transaction information.

5.3 Third-Party Service Providers

The Company may utilise approved third-party payment providers and other service providers to facilitate cryptocurrency payment processing.

The use of third-party providers does not transfer or reduce the Company's regulatory responsibilities.

The Company remains fully responsible for ensuring that all cryptocurrency activities conducted under its Curaçao gaming licence comply with applicable legislation, the CGA requirements, AML/CFT obligations and this Policy.

Third-party providers shall be subject to appropriate due diligence, ongoing oversight and periodic review in accordance with the Company's Vendor Due Diligence procedures and applicable regulatory requirements.

6. Cryptocurrency Risk Management Principles

The Company recognises that virtual assets present higher inherent risks than traditional payment methods due to their cross-border nature, technological complexity and potential exposure to money laundering, terrorist financing, sanctions evasion, fraud and other financial crime.

Accordingly, all cryptocurrency-related activities shall be managed using a documented risk-based approach designed to identify, assess, mitigate and continuously monitor the risks associated with the acceptance and processing of virtual assets.

The following principles govern the Company's cryptocurrency risk management framework.

6.1 Risk-Based Approach

All cryptocurrency transactions shall be subject to a risk-based assessment taking into consideration, where applicable:

- the type of cryptocurrency involved;
- the customer's risk profile;
- the source of funds;
- wallet characteristics;
- transaction behaviour;
- geographic risk;
- sanctions exposure;
- any other relevant financial crime indicators.

Higher-risk transactions shall be subject to enhanced review and additional due diligence measures in accordance with the Company's AML/CFT Policy and Enhanced Due Diligence Procedure.

6.2 Regulatory Compliance

The Company shall ensure that cryptocurrency activities remain fully compliant with:

- applicable Curaçao legislation;
- CGA Policy Guidelines;
- AML/CFT requirements;
- sanctions obligations;
- internal compliance policies and procedures.

Where regulatory requirements change, this Policy and the associated operational procedures shall be reviewed and updated accordingly.

6.3 Transparency and Traceability

The Company shall only process cryptocurrency transactions where sufficient transparency and traceability can be maintained.

Cryptocurrency assets, wallet structures or transaction mechanisms that prevent effective monitoring, customer identification or source-of-funds verification shall not be accepted.

6.4 Ongoing Transaction Monitoring

Cryptocurrency transactions shall be subject to ongoing monitoring throughout the customer relationship.

The Company shall apply appropriate monitoring controls designed to identify unusual transaction patterns, elevated risk indicators, sanctions exposure and other circumstances requiring further investigation or escalation.

Where appropriate, additional customer due diligence measures may be applied prior to processing transactions.

6.5 Proportionality

Risk controls implemented under this Policy shall remain proportionate to:

- the products offered;
- the cryptocurrencies accepted;
- the transaction volumes;
- the Company's operational model;
- the overall financial crime risk exposure.

The Company shall periodically reassess whether existing controls remain appropriate and effective.

6.6 Continuous Improvement

The Company is committed to continuously improving its cryptocurrency governance framework.

Risk assessments, internal controls, transaction monitoring procedures and operational practices shall be reviewed periodically to reflect:

- regulatory developments;
- emerging financial crime typologies;
- technological developments;
- operational experience;
- lessons learned from internal reviews, incidents or audits.

7. Approved Crypto Assets and Prohibited Assets

7.1 Approved Crypto Assets

The Company shall only accept cryptocurrencies that have been subject to an internal risk assessment and formally approved for use within the licensed operation.

When determining whether a cryptocurrency may be accepted, the Company shall consider, among other factors:

- regulatory expectations and legal requirements;
- market maturity and liquidity;
- blockchain transparency and traceability;
- availability of blockchain analytics and transaction monitoring capabilities;
- sanctions and financial crime exposure;
- operational and security considerations;
- customer demand and business requirements.

The list of cryptocurrencies approved for use by the Company is maintained in **Annex A – Approved Cryptocurrencies**.

Any addition, removal or restriction of a cryptocurrency shall be supported by a documented risk assessment and approved in accordance with the Company's governance procedures.

7.2 Stablecoins

The Company recognises that fiat-backed stablecoins generally present lower volatility than many other crypto-assets and may therefore provide greater stability for payment processing.

Where stablecoins are accepted, they shall remain subject to the same AML/CFT, transaction monitoring, sanctions screening and risk assessment requirements applicable to all other supported cryptocurrencies.

7.3 Prohibited Crypto Assets

The Company shall not accept cryptocurrencies or digital assets where effective monitoring, traceability or regulatory compliance cannot be reasonably achieved.

Without limitation, the following categories are prohibited:

- cryptocurrencies designed primarily to conceal transaction history or wallet ownership through privacy-enhancing technologies;
- cryptocurrency transactions originating from or associated with sanctioned wallets;
- cryptocurrency transactions involving sanctioned mixers or tumblers;
- wrapped tokens or bridged assets where the provenance of the underlying asset cannot be reasonably established;
- cryptocurrency assets or transaction mechanisms prohibited by the Curaçao Gaming Authority or applicable legislation.

Examples of prohibited or restricted privacy-enhancing cryptocurrencies include, but are not limited to:

- Monero (XMR);
- Zcash (shielded transactions);
- Dash (where privacy functionality is utilised);
- Litecoin MWEB transactions where privacy features are enabled.

The Company reserves the right to prohibit additional cryptocurrencies where their risk profile is considered unacceptable or where required by applicable legislation or regulatory guidance.

7.4 Periodic Review

The list of approved cryptocurrencies contained in **Annex A** shall be reviewed periodically and updated whenever new cryptocurrencies are introduced, existing cryptocurrencies are removed, or the Company's risk assessment identifies material changes affecting their suitability.

All changes shall be appropriately documented and approved in accordance with the Company's governance framework.

8. Approved Crypto Payment Providers

8.1 General Principles

The Company may utilise approved third-party cryptocurrency payment providers and Virtual Asset Service Providers (VASPs) to facilitate cryptocurrency payment processing in connection with its licensed gaming operations.

The use of third-party providers does not transfer, reduce or limit the Company's regulatory responsibilities. K.I.K. Corporation B.V. remains fully responsible for ensuring compliance with all applicable legal, regulatory and licensing requirements relating to cryptocurrency transactions conducted under its Curaçao gaming licence.

Only payment providers that have undergone an appropriate due diligence assessment and have been formally approved by the Company may be used for cryptocurrency payment processing.

The list of approved cryptocurrency payment providers is maintained in **Annex B – Approved Crypto Payment Providers (VASPs)**.

8.2 Due Diligence Requirements

Prior to engaging a cryptocurrency payment provider or Virtual Asset Service Provider (VASP), the Company shall conduct appropriate due diligence, taking into consideration, where applicable:

- regulatory or licensing status within its home jurisdiction;
- AML/CFT compliance framework;
- sanctions screening capabilities;
- transaction monitoring capabilities;
- wallet security controls;
- Travel Rule capabilities, where applicable;
- operational resilience and business continuity arrangements;
- reputation and market standing;
- information security standards;
- contractual arrangements governing the services provided.

The extent of due diligence shall be proportionate to the level of risk associated with the services provided.

8.3 Ongoing Monitoring

Approved cryptocurrency payment providers shall be subject to periodic review to ensure that they continue to satisfy the Company's operational, compliance and regulatory expectations.

The Company may conduct additional reviews where:

- material changes occur within the provider's business;
- significant regulatory developments arise;
- security incidents are identified;
- deficiencies in AML/CFT controls become apparent;
- other circumstances increase the Company's exposure to financial crime or operational risk.

Where appropriate, the Company may suspend or terminate the use of a provider where continued use would expose the licensed operation to unacceptable regulatory, operational or financial crime risks.

8.4 Outsourced Services

Where cryptocurrency payment processing is outsourced, the Company shall maintain appropriate oversight over the outsourced activities.

Outsourcing arrangements shall not affect the Company's responsibility to:

- maintain effective AML/CFT controls;
- monitor cryptocurrency transactions;
- conduct customer due diligence where required;
- investigate suspicious activity;
- comply with applicable reporting obligations;
- protect customer funds and information;
- comply with all applicable CGA requirements.

9. Wallet Governance

9.1 General Principles

The Company shall ensure that all cryptocurrency wallets used in connection with its licensed gaming operations are managed in a secure, controlled and transparent manner.

Wallet management practices shall be designed to protect customer assets, support regulatory compliance, maintain operational integrity and minimise the risk of fraud, theft, unauthorised access or misuse.

The Company shall maintain appropriate governance over all cryptocurrency wallets used within the licensed operation, irrespective of whether such wallets are operated directly by the Company or through an approved cryptocurrency payment provider.

The Company's wallet governance framework is described in **Annex C – Wallet Governance Framework**.

9.2 Approved Wallet Arrangements

Only wallet arrangements approved by the Company and supported by authorised cryptocurrency payment providers may be used for processing cryptocurrency transactions.

Wallet infrastructure shall be established in accordance with operational, security and regulatory requirements and shall support:

- secure receipt of customer deposits;
- secure processing of withdrawals;
- transaction traceability;
- record retention;

- AML/CFT monitoring;
- sanctions compliance.

9.3 Wallet Security

Appropriate technical and organisational measures shall be implemented to protect cryptocurrency wallets against unauthorised access, compromise or loss.

Where applicable, wallet security measures may include:

- multi-factor authentication;
- role-based access controls;
- segregation of duties;
- multi-signature authorisation or equivalent approval mechanisms;
- secure credential management;
- encryption of sensitive information;
- periodic security reviews.

The specific security controls implemented may vary depending on the wallet architecture and the services provided by approved third-party payment providers.

9.4 Access Management

Access to cryptocurrency wallet administration functions shall be restricted to authorised personnel whose responsibilities require such access.

Access rights shall be granted on the basis of the principle of least privilege and shall be reviewed periodically.

Any changes to access permissions shall be appropriately authorised and documented.

9.5 Operational Oversight

The Company shall maintain appropriate oversight over wallet operations, including:

- monitoring wallet activity;
- reviewing operational exceptions;
- investigating irregular transactions;
- supporting reconciliation activities;
- maintaining appropriate audit trails.

Where wallet services are provided by an approved third-party payment provider, the Company shall maintain oversight through contractual arrangements, operational reporting and ongoing due diligence.

9.6 Periodic Review

Wallet governance arrangements shall be reviewed periodically and whenever there are significant operational, regulatory or technological changes.

Where deficiencies or new risks are identified, appropriate corrective measures shall be implemented without undue delay.

10. AML/CFT Controls

10.1 General Principles

The Company applies a risk-based AML/CFT framework to all cryptocurrency-related activities conducted under its Curaçao gaming licence.

Cryptocurrency transactions are subject to the same AML/CFT principles applicable to fiat transactions, together with additional controls designed to address the specific risks associated with virtual assets.

The Company's AML/CFT framework is supported by its AML/CFT Policy, Business Risk Assessment, Customer Risk Assessment Methodology, Enhanced Due Diligence (EDD) Procedure, Transaction Monitoring Procedures and other related compliance policies.

10.2 Risk-Based Approach

The Company applies a risk-based approach when assessing cryptocurrency customers and transactions.

Risk assessments may take into consideration, where applicable:

- customer profile;
- jurisdictional risk;
- transaction value and frequency;
- type of cryptocurrency used;
- wallet characteristics;
- source of funds;
- sanctions exposure;
- blockchain analytics results;
- any other relevant financial crime indicators.

Higher-risk customers or transactions shall be subject to additional review and enhanced due diligence measures.

10.3 Customer Due Diligence

Customers using cryptocurrency payment methods shall remain subject to the Company's customer due diligence requirements.

The Company shall perform customer identification and verification in accordance with applicable legislation and its internal AML/CFT procedures.

Additional verification measures may be applied where cryptocurrency-related risks are considered elevated.

10.4 Enhanced Due Diligence

Enhanced Due Diligence (EDD) shall be performed where required under the Company's EDD Procedure or where cryptocurrency activity presents an increased level of risk.

EDD measures may include, where appropriate:

- obtaining additional information regarding the customer;
- verification of source of funds or source of wealth;
- verification of wallet ownership;
- enhanced review of transaction history;
- management approval before continuing the business relationship;
- ongoing enhanced monitoring.

10.5 Sanctions Compliance

All cryptocurrency transactions shall remain subject to applicable sanctions screening requirements.

The Company shall take reasonable measures to identify transactions involving sanctioned persons, entities or cryptocurrency wallets and shall take appropriate action where sanctions concerns are identified.

Where required, transactions may be delayed, rejected, suspended or escalated pending further review.

10.6 Suspicious Activity

Where cryptocurrency activity gives rise to reasonable suspicion of money laundering, terrorist financing, sanctions evasion, fraud or any other criminal activity, the matter shall be escalated to the Compliance Officer without undue delay.

The Compliance Officer shall assess the circumstances and determine whether additional due diligence, internal investigation or external reporting is required in

accordance with applicable legislation and the Company's internal reporting procedures.

10.7 Record Retention

All AML/CFT documentation relating to cryptocurrency transactions, including customer due diligence records, monitoring results, investigations and supporting evidence, shall be retained in accordance with applicable legal and regulatory requirements and the Company's Record Retention Policy.

11. Blockchain Analytics and Transaction Monitoring

11.1 General Principles

The Company applies appropriate monitoring controls to cryptocurrency transactions in order to identify, assess and manage financial crime risks associated with virtual assets.

Cryptocurrency transaction monitoring forms part of the Company's overall AML/CFT framework and is conducted using a risk-based approach supported by internal procedures and, where applicable, the capabilities of approved cryptocurrency payment providers and other authorised service providers.

The objective of transaction monitoring is to identify unusual, suspicious or high-risk activity that may require further review, enhanced due diligence or escalation.

11.2 Blockchain Analytics

Where appropriate, blockchain analytics tools and services may be utilised to assist in assessing cryptocurrency transactions and wallet activity.

Blockchain analytics may support the identification of:

- sanctioned wallets or addresses;
- exposure to illicit or high-risk activities;
- links to known fraud, ransomware or darknet activity;
- unusual transaction patterns;
- wallet risk indicators;
- other financial crime risks relevant to cryptocurrency transactions.

The Company shall consider the outcome of such assessments as part of its overall risk evaluation and decision-making process.

11.3 Transaction Monitoring

Cryptocurrency transactions shall be subject to ongoing monitoring throughout the customer relationship.

Monitoring activities may include, where applicable:

- review of transaction frequency;
- review of transaction values;
- customer behavioural analysis;
- monitoring of wallet activity;
- identification of unusual transaction patterns;
- review of repeated or structured transactions;
- monitoring of customer risk profiles;
- review of transactions involving higher-risk jurisdictions.

Transaction monitoring shall be performed in accordance with the Company's Transaction Monitoring Procedures and AML/CFT Policy.

11.4 Alerts and Escalation

Where monitoring activities identify elevated risk indicators or unusual activity, the matter shall be escalated for further assessment.

Depending on the nature of the identified risk, appropriate actions may include:

- additional customer due diligence;
- Enhanced Due Diligence (EDD);
- verification of wallet ownership;
- requests for supporting documentation;
- temporary suspension of transaction processing;
- internal investigation;
- escalation to the Compliance Officer;
- consideration of regulatory reporting obligations where applicable.

11.5 Ongoing Review

Monitoring activities shall continue throughout the customer relationship and shall not be limited to onboarding.

The Company shall periodically review the effectiveness of its cryptocurrency monitoring controls and make appropriate improvements where new risks, technologies or regulatory expectations emerge.

11.6 Documentation

Monitoring activities, investigations, decisions and escalation outcomes shall be appropriately documented and retained in accordance with the Company's record retention requirements.

Documentation shall be sufficient to demonstrate the basis for decisions taken in relation to cryptocurrency transactions and to support regulatory review where required.

12. Customer and Wallet Verification

12.1 General Principles

The Company shall take appropriate measures to verify the identity of its customers and, where applicable, the ownership or control of cryptocurrency wallets used in connection with its licensed gaming operations.

Customer and wallet verification measures form part of the Company's overall AML/CFT framework and are designed to reduce the risks associated with money laundering, terrorist financing, sanctions evasion, fraud and other financial crime.

Customer verification requirements shall be applied in accordance with the Company's AML/CFT Policy, while additional wallet-related verification measures shall be applied on a risk-based basis where appropriate.

12.2 Customer Verification

Customers using cryptocurrency payment methods shall remain subject to the same customer identification and verification requirements applicable to all other payment methods.

The use of cryptocurrency shall not exempt any customer from applicable KYC, Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) or ongoing monitoring requirements.

Additional verification measures may be applied where the customer's risk profile or transaction activity warrants further assessment.

12.3 Wallet Verification

Where considered necessary based on the Company's risk assessment, additional verification may be performed to establish that a customer owns or controls the cryptocurrency wallet used for transactions.

Wallet verification measures may include, where appropriate:

- verification through the approved cryptocurrency payment provider;
- confirmation of wallet ownership using appropriate technical or operational methods;
- review of supporting customer information;
- verification during Enhanced Due Diligence procedures;
- any other reasonable verification method considered appropriate by the Company.

The extent of wallet verification shall be proportionate to the level of identified risk.

12.4 Hosted and Unhosted Wallets

The Company recognises that customers may utilise either hosted wallets provided by regulated Virtual Asset Service Providers (VASPs) or unhosted (self-hosted) wallets under their own control.

Transactions involving unhosted wallets may present additional financial crime risks and may therefore be subject to enhanced review, additional verification or further due diligence where considered necessary.

The Company shall assess such transactions on a risk-based basis, taking into consideration applicable regulatory expectations and internal risk assessment procedures.

12.5 Verification Outcomes

Where customer or wallet verification cannot be satisfactorily completed, or where material inconsistencies, elevated risks or suspicious indicators are identified, the Company may, where appropriate:

- request additional information or documentation;
- apply Enhanced Due Diligence measures;
- delay or decline the processing of a cryptocurrency transaction;
- restrict or suspend account activity;
- escalate the matter to the Compliance Officer for further assessment;
- take any other action required under applicable legislation or the Company's internal policies.

12.6 Documentation

All customer and wallet verification activities, supporting documentation and decisions shall be appropriately recorded and retained in accordance with the Company's Record Retention Policy and applicable legal and regulatory requirements.

13. Cryptocurrency Deposits

13.1 General Principles

The Company permits customers of **232Casino** to fund their gaming accounts using approved cryptocurrencies supported by the Company's authorised cryptocurrency payment provider(s).

Cryptocurrency deposits shall be processed in accordance with this Policy, the Company's AML/CFT framework and all applicable legal and regulatory requirements.

Only cryptocurrencies approved by the Company and listed in **Annex A – Approved Cryptocurrencies** may be accepted.

13.2 Deposit Processing

Cryptocurrency deposits shall be processed exclusively through approved cryptocurrency payment providers authorised by the Company.

The Company shall implement appropriate operational controls to ensure that cryptocurrency deposits are:

- accurately received;
- appropriately recorded;
- allocated to the correct customer account;
- subject to applicable AML/CFT monitoring;
- retained within the Company's transaction records.

13.3 Risk Assessment

Cryptocurrency deposits shall be assessed using a risk-based approach.

Where appropriate, deposits may be subject to additional review taking into consideration:

- customer risk profile;
- transaction value;
- transaction frequency;
- blockchain-related risk indicators;
- sanctions exposure;
- wallet characteristics;
- unusual transaction behaviour;
- other relevant financial crime indicators.

13.4 Source of Funds

Where required under the Company's AML/CFT framework, customers may be requested to provide additional information regarding the source of funds used for cryptocurrency deposits.

The extent of such enquiries shall be proportionate to the level of identified risk and shall be conducted in accordance with the Company's Enhanced Due Diligence Procedure.

13.5 Refusal of Deposits

The Company reserves the right to reject, suspend or delay the processing of cryptocurrency deposits where:

- regulatory requirements so require;
- customer verification cannot be satisfactorily completed;
- sanctions concerns are identified;
- suspicious activity is detected;
- the cryptocurrency or wallet presents an unacceptable level of risk;
- acceptance of the transaction would otherwise expose the Company to unacceptable regulatory, operational or financial crime risks.

13.6 Record Keeping

Information relating to cryptocurrency deposits shall be retained in accordance with the Company's Record Retention Policy and applicable legal and regulatory requirements.

14. Cryptocurrency Withdrawals

14.1 General Principles

The Company permits eligible customers to withdraw funds using approved cryptocurrencies, subject to compliance with this Policy, the Company's AML/CFT framework and all applicable legal and regulatory requirements.

All withdrawal requests shall be assessed using a risk-based approach designed to protect the integrity of the licensed operation and mitigate money laundering, terrorist financing, fraud, sanctions and other financial crime risks.

14.2 Withdrawal Processing

Cryptocurrency withdrawals shall be processed only through the Company's approved cryptocurrency payment provider(s).

Prior to processing a withdrawal, the Company may perform appropriate verification and review procedures, taking into consideration:

- customer verification status;
- customer risk profile;
- transaction history;
- account activity;
- wallet-related risk indicators;
- AML/CFT requirements;
- sanctions screening results;
- any other relevant risk factors.

14.3 Withdrawal Wallet Assessment

The Company recognises that withdrawal requests may involve cryptocurrency wallets different from those previously used by the customer.

Where a withdrawal is requested to a different wallet, additional review or verification may be performed where considered appropriate based on the Company's risk assessment.

The use of a different wallet shall not automatically result in the rejection of a withdrawal request, provided that the Company is satisfied that the identified risks have been appropriately assessed and mitigated.

14.4 Withdrawal Asset Assessment

The Company recognises that customers may request withdrawals using a cryptocurrency different from the cryptocurrency originally used for deposit, where such functionality is available through the Company's approved cryptocurrency payment provider.

Requests involving a different withdrawal asset shall be assessed using a risk-based approach, taking into consideration the customer's transaction history, wallet verification status, AML/CFT requirements, operational considerations and any other relevant risk indicators.

The use of a different cryptocurrency for withdrawal shall not automatically result in the rejection of a withdrawal request. The Company shall assess such requests on a case-by-case basis and may approve, request additional information or decline the transaction where necessary to ensure compliance with applicable legal, regulatory and internal requirements.

14.5 Enhanced Review

Additional review or Enhanced Due Diligence may be applied where cryptocurrency withdrawal activity presents elevated financial crime or operational risks.

Examples may include:

- significant changes in customer transaction behaviour;
- unusual withdrawal patterns;
- high-value transactions;
- higher-risk jurisdictions;
- elevated wallet risk indicators;
- sanctions-related concerns;
- other circumstances identified through the Company's risk assessment.

14.6 Refusal or Suspension of Withdrawals

The Company reserves the right to delay, suspend or decline cryptocurrency withdrawals where:

- customer verification requirements have not been satisfactorily completed;
- additional due diligence is required;
- sanctions concerns are identified;
- suspicious activity is detected;
- regulatory requirements so require;
- processing the withdrawal would expose the Company to unacceptable legal, regulatory or operational risks.

Any such decision shall be appropriately documented and, where applicable, reviewed by the Compliance Officer.

14.7 Record Keeping

All cryptocurrency withdrawal requests, reviews, approvals, refusals and supporting documentation shall be retained in accordance with the Company's Record Retention Policy and applicable legal and regulatory requirements.

15. Incident Reporting

15.1 General Principles

The Company shall ensure that all cryptocurrency-related incidents are identified, assessed, documented and managed in a timely and appropriate manner.

Cryptocurrency incidents shall be handled in accordance with the Company's Incident Reporting Procedure, Information Security Policy, AML/CFT framework and other applicable internal policies.

The objective of incident reporting is to minimise operational disruption, protect customer assets, maintain regulatory compliance and support the integrity of the Company's licensed gaming operations.

15.2 Reportable Incidents

Cryptocurrency-related incidents may include, but are not limited to:

- suspected or confirmed unauthorised access to cryptocurrency wallets or related systems;
- suspected fraud or attempted fraud involving cryptocurrency transactions;
- cybersecurity incidents affecting cryptocurrency payment processing;
- operational failures impacting cryptocurrency deposits or withdrawals;
- suspected sanctions violations;
- suspicious cryptocurrency transactions requiring investigation;
- failures or disruptions involving approved cryptocurrency payment providers;
- blockchain-related events affecting the Company's cryptocurrency operations;
- any other event that may expose the Company to legal, regulatory, financial or operational risk.

Examples of cryptocurrency incident categories are maintained in **Annex E – Crypto Incident Categories**.

15.3 Internal Reporting

Employees shall promptly report any actual or suspected cryptocurrency-related incident through the Company's established internal reporting channels.

Reported incidents shall be assessed by the appropriate personnel and escalated where necessary to the Compliance Officer, senior management, Information Technology personnel or other responsible functions, depending on the nature of the incident.

15.4 Investigation and Response

The Company shall investigate cryptocurrency-related incidents in a timely manner and implement appropriate corrective actions to mitigate identified risks.

Depending on the nature and severity of the incident, response measures may include:

- suspension of affected transactions;

- additional customer verification;
- Enhanced Due Diligence (EDD);
- technical investigation;
- coordination with approved cryptocurrency payment providers;
- implementation of corrective or preventive measures;
- consideration of regulatory reporting obligations where required.

15.5 Regulatory Reporting

Where required by applicable legislation or regulatory requirements, cryptocurrency-related incidents shall be reported to the appropriate competent authority within the applicable reporting timeframes.

The Compliance Officer shall assess whether an incident gives rise to any external reporting obligation and shall coordinate such reporting where necessary.

15.6 Incident Documentation

All cryptocurrency-related incidents, investigations, decisions, corrective actions and lessons learned shall be appropriately documented and retained in accordance with the Company's Record Retention Policy.

Where appropriate, identified control weaknesses shall be incorporated into future risk assessments, policy reviews and staff training.

16. Record Keeping

16.1 General Principles

The Company shall maintain complete, accurate and reliable records relating to all cryptocurrency activities conducted under its Curaçao gaming licence.

Records shall be retained in a manner that supports regulatory compliance, financial crime investigations, internal oversight, audit activities and business continuity.

Record retention shall be performed in accordance with applicable legal and regulatory requirements and the Company's Record Retention Policy.

16.2 Records Maintained

The Company shall maintain, where applicable, records relating to:

- customer identification and verification;
- customer due diligence and Enhanced Due Diligence (EDD);

- cryptocurrency deposits and withdrawals;
- transaction monitoring activities;
- blockchain analytics and risk assessments;
- wallet verification activities;
- sanctions screening results;
- suspicious activity reviews and investigations;
- incident reports and corrective actions;
- communications relating to cryptocurrency transactions where relevant;
- approvals, exceptions and escalation decisions;
- approved cryptocurrency payment providers, including due diligence, contractual arrangements, periodic reviews and other documentation relevant to the Company's oversight responsibilities, where applicable.

16.3 Integrity and Security of Records

Cryptocurrency-related records shall be protected against unauthorised access, alteration, loss or destruction.

Appropriate technical and organisational measures shall be implemented to ensure:

- confidentiality;
- integrity;
- availability;
- authenticity;
- traceability of records.

Access to cryptocurrency-related records shall be restricted to authorised personnel with legitimate business or regulatory responsibilities.

16.4 Availability of Records

Cryptocurrency-related records shall be maintained in a manner that enables timely retrieval for:

- internal reviews;
- compliance monitoring;
- internal and external audits;
- regulatory inspections;
- investigations by competent authorities.

16.5 Record Retention Period

Cryptocurrency-related records shall be retained for the period prescribed by applicable legislation, regulatory requirements and the Company's Record Retention Policy.

Where multiple retention requirements apply, the Company shall retain records for the longer applicable period unless otherwise required by law.

16.6 Disposal of Records

Upon expiry of the applicable retention period, records shall be securely disposed of in accordance with the Company's Record Retention Policy and Information Security Policy.

Where litigation, regulatory investigations or other legal proceedings are pending or reasonably anticipated, relevant records shall be preserved until such matters have been concluded or otherwise authorised for disposal.

17. Training and Awareness

17.1 General Principles

The Company recognises that effective governance of cryptocurrency activities requires appropriately trained personnel with an understanding of the risks associated with virtual assets and the Company's regulatory obligations.

Employees whose responsibilities involve cryptocurrency-related activities shall receive appropriate training relevant to their roles.

17.2 Training Programme

The Company's cryptocurrency training programme shall be proportionate to the nature of the employee's responsibilities and may include, where applicable:

- the requirements of this Crypto Policy;
- applicable legal and regulatory obligations;
- AML/CFT risks associated with cryptocurrency transactions;
- customer due diligence and Enhanced Due Diligence requirements;
- transaction monitoring principles;
- wallet verification principles;
- sanctions awareness;
- fraud indicators;
- incident reporting procedures;
- information security requirements;
- escalation procedures.

Training content shall be reviewed periodically to reflect regulatory developments, emerging financial crime typologies and operational changes.

17.3 Target Audience

Cryptocurrency-related training shall be provided, as appropriate, to personnel involved in:

- Compliance;
- Finance;
- Operations;
- Customer Support;
- Information Technology;
- Management;
- any other personnel whose responsibilities involve cryptocurrency activities.

Training shall be appropriate to the responsibilities of each function.

17.4 Refresher Training

Refresher training shall be provided periodically and whenever significant legislative, regulatory, technological or operational changes affect the Company's cryptocurrency activities.

Additional training may be provided following significant incidents, audit findings, policy updates or the introduction of new cryptocurrency products or services.

17.5 Training Records

The Company shall maintain appropriate records of cryptocurrency-related training, including attendance, training materials and, where applicable, evidence of completion.

Training records shall be retained in accordance with the Company's Record Retention Policy.

18. Policy Review and Continuous Improvement

18.1 Policy Review

This Policy shall be reviewed periodically to ensure that it remains appropriate, effective and aligned with the Company's cryptocurrency activities, applicable legal and regulatory requirements, and industry best practices.

As a minimum, this Policy shall be reviewed annually or earlier where required due to:

- legislative or regulatory changes;

- amendments to applicable CGA requirements or guidance;
- material changes to the Company's cryptocurrency activities;
- significant operational or technological developments;
- changes affecting approved cryptocurrency payment providers or wallet arrangements;
- findings arising from internal reviews, audits or regulatory inspections;
- significant cryptocurrency-related incidents.

Where appropriate, this Policy shall be updated following completion of the review.

18.2 Continuous Improvement

The Company is committed to the continuous enhancement of its cryptocurrency governance framework.

The effectiveness of the Company's cryptocurrency controls shall be evaluated on an ongoing basis, taking into consideration:

- emerging financial crime typologies;
- developments in blockchain technology;
- evolving regulatory expectations;
- industry guidance and best practices;
- operational experience;
- internal audit findings;
- compliance monitoring results;
- lessons learned from incidents and investigations.

Where improvements are identified, the Company shall implement appropriate corrective or preventive measures in accordance with its governance framework.

18.3 Review of Supporting Documentation

Where changes to this Policy affect associated internal documentation, the Company shall ensure that related policies and procedures are reviewed and updated as appropriate.

This may include, where applicable:

- AML/CFT Policy;
- Business Risk Assessment;
- Enhanced Due Diligence Procedure;
- Transaction Monitoring Procedures;
- Incident Reporting Procedure;
- Information Security Policy;
- Operations Manual;
- other related compliance documentation.

18.4 Review of Annexes

The Annexes forming part of this Policy shall be reviewed periodically to ensure that they accurately reflect the Company's current cryptocurrency operations and approved governance arrangements.

Where operational changes occur, including but not limited to changes to approved cryptocurrencies, cryptocurrency payment providers, wallet governance arrangements or implementation milestones, the relevant Annex(es) shall be updated following the Company's internal approval process.

Updates to the Annexes shall not require amendment of the main body of this Policy unless such changes materially affect the Company's governance framework or regulatory obligations.

19. Document Control

19.1 Ownership

This Policy is owned by **K.I.K. Corporation B.V.** and forms part of the Company's overall governance and compliance framework.

The Compliance Officer is responsible for coordinating the review, maintenance and implementation of this Policy, while the Board of Directors retains ultimate responsibility for its approval.

19.2 Approval

This Policy shall be approved by the Board of Directors prior to implementation.

Any material amendments to this Policy shall be subject to appropriate internal review and approval in accordance with the Company's governance framework.

19.3 Distribution

This Policy shall be made available to relevant personnel whose responsibilities involve cryptocurrency-related activities.

The Company shall ensure that only the current approved version of this Policy is used for operational and compliance purposes.

Superseded versions shall be appropriately archived and retained in accordance with the Company's Record Retention Policy.

19.4 Document Amendments

This Policy may be amended where necessary to reflect:

- legislative or regulatory changes;
- amendments to CGA guidance;
- changes to the Company's cryptocurrency operations;
- changes to internal governance arrangements;
- audit findings;
- compliance monitoring outcomes;
- operational improvements;
- any other material developments affecting cryptocurrency activities.

Material amendments shall be documented through the Company's document control process.

19.5 Relationship with Other Policies

This Policy shall be read together with the Company's:

- AML/CFT Policy;
- Business Risk Assessment;
- Enhanced Due Diligence Procedure;
- Transaction Monitoring Procedures;
- Incident Reporting Procedure;
- Information Security Policy;
- Operations Manual;
- Record Retention Policy; and
- other applicable governance and compliance documentation.

Where inconsistencies arise, applicable legislation and regulatory requirements shall prevail.

19.6 Annexes

The Annexes attached to this Policy form an integral part of the Company's Crypto Policy.

Each Annex shall be maintained under the Company's document governance process and reviewed periodically to ensure continued accuracy and relevance.

Operational updates to the Annexes may be approved independently where such updates do not materially affect the principles, governance framework or regulatory obligations established by this Policy.

ANNEX A – Approved Cryptocurrencies

Purpose

This Annex contains the list of cryptocurrencies approved for use within the Company's licensed gaming operations.

Only cryptocurrencies included in this Annex may be accepted for deposits and/or withdrawals.

The list shall be reviewed periodically and updated following documented internal approval.

Cryptocurrency	Symbol	Network	Deposits	Withdrawals	Status
Bitcoin	BTC	Bitcoin	✓	✓	Approved
Ethereum	ETH	Ethereum	✓	✓	Approved
Litecoin	LTC	Litecoin	✓	✓	Approved
Bitcoin Cash	BCH	Bitcoin Cash	✓	✓	Approved
Solana	SOL	Solana	✓	✓	Approved
Binance Coin	BNB	BNB Smart Chain	✓	✓	Approved
Dogecoin	DOGE	Dogecoin	✓	✓	Approved
TRON	TRX	Tron	✓	✓	Approved
Tether	USDT	Ethereum (ERC-20)	✓	✓	Approved
Tether	USDT	Tron (TRC-20)	✓	✓	Approved
Tether	USDT	BNB Smart Chain (BEP-20)	✓	✓	Approved
USD Coin	USDC	Ethereum (ERC-20)	✓	✓	Approved
USD Coin	USDC	Solana	✓	✓	Approved

Review Frequency

This Annex shall be reviewed periodically and whenever:

- a new cryptocurrency is introduced;
- support for an existing cryptocurrency is discontinued;
- regulatory requirements change;
- the Company's risk assessment identifies material changes.

ANNEX B – Approved Crypto Payment Providers (VASPs)

Approved Providers

Provider	Service	Contracting Entity	Licensed Entity	Jurisdiction	Status
CoinsPaid (via Dream Finance Processing Inc.)	Cryptocurrency payment processing	Holzman Limited	K.I.K. Corporation B.V.	Alberta, Canada	Approved

Services

The approved provider currently supports:

- cryptocurrency deposits;
 - cryptocurrency withdrawals;
 - wallet management services;
 - blockchain transaction processing;
 - operational support for approved cryptocurrencies.
-

Periodic Review

The Company shall periodically review:

- contractual arrangements;
- regulatory status;
- operational performance;
- AML/CFT capabilities;
- security standards;
- business continuity arrangements.

ANNEX C – Wallet Governance Framework

Wallet Types

The Company's cryptocurrency operations may utilise wallet arrangements provided by approved cryptocurrency payment providers.

Wallet infrastructure may include:

- Deposit Wallets
- Withdrawal Wallets
- Operational Wallets
- Treasury Wallets
- Hot Wallets
- Cold Wallets (where applicable)

Wallet architecture is maintained by the approved payment provider and is subject to appropriate operational oversight by the Company.

Wallet Governance Principles

- secure wallet management;
- segregation of duties;
- restricted access;
- transaction traceability;
- audit logging;
- periodic review.

ANNEX D – Wallet Verification Methods

Depending on the level of identified risk, wallet ownership verification may include:

- verification through the approved payment provider;
- confirmation of wallet ownership;
- supporting customer documentation;
- Enhanced Due Diligence (EDD);
- additional verification where considered appropriate.

Verification measures shall be proportionate to the level of identified risk.

ANNEX E – Crypto Incident Categories

Examples of reportable cryptocurrency-related incidents include:

Operational

- Failed deposits
- Failed withdrawals
- Provider outage
- Blockchain congestion

Security

- Wallet compromise
- Unauthorized access
- Credential compromise
- Suspicious login activity

AML / Compliance

- Sanctions exposure
- Suspicious wallet
- High-risk blockchain activity
- Transaction requiring investigation

Fraud

- Identity fraud
- Account takeover
- Payment abuse
- Bonus abuse involving cryptocurrency

Regulatory

- Regulatory reporting event
- Material compliance breach
- Failure to comply with regulatory obligations

ANNEX F – Implementation Roadmap

Requirement	Target Date	Status
Crypto Policy	September 2026	Pending Submission
Internal review and approval	September 2026	Planned
Upload to CGA Portal	September 2026	Planned
Staff awareness training	December 2026	Planned
Additional crypto risk assessment enhancements	December 2026	Planned
Ongoing implementation of operational controls	June 2027	Planned

ANNEX G – Crypto Asset Risk Assessment Matrix

Cryptocurrency	Risk Level	Rationale
BTC	Medium	High liquidity and strong blockchain transparency.
ETH	Medium	Widely accepted with established monitoring capabilities.
LTC	Medium	Mature blockchain with available analytics.
BCH	Medium	Mature blockchain with available analytics.
SOL	Medium	Supported by approved provider and available monitoring tools.
BNB	Medium	Supported by approved provider and available monitoring tools.
DOGE	Medium	Accepted through approved provider; monitored using existing AML controls.
TRX	Medium	Supported by approved provider and subject to transaction monitoring.
USDT	Medium	Fiat-backed stablecoin; accepted only through approved networks and payment provider.
USDC	Low-Medium	Fiat-backed stablecoin with strong market acceptance and monitoring capabilities.
Privacy Coins (e.g. Monero, shielded Zcash)	High / Prohibited	Not supported due to limited transaction transparency and elevated AML/CFT risk.