

TRUSTDICE

CRYPTOCURRENCY & DIGITAL ASSET

POLICY

Document Control

- Version: 1.0
- Effective Date: [2026/07/20]
- Review Date: [2027/07/20]

1. PURPOSE

The purpose of this Cryptocurrency & Digital Asset Policy ("Policy") is to establish the governance framework, operational standards, and internal controls governing the acceptance, storage, transfer, safeguarding, monitoring, and management of cryptocurrencies used within the licensed gaming operations of **Satoshi Gaming Group N.V.** ("the Operator").

This Policy has been developed in accordance with the applicable requirements of the Curaçao National Ordinance on Games of Chance (LOK), the Curaçao Gaming Authority ("CGA") Crypto Policy Guideline for Online Gaming Operators, the Operator's AML/CFT Policy, Responsible Gaming Policy, Information Security Policy, and other applicable internal governance documents. It is intended to ensure that the Operator maintains appropriate standards of player protection, financial crime prevention, operational resilience, and digital asset security.

As the Operator conducts its gaming business exclusively through cryptocurrencies, this Policy establishes a comprehensive framework covering the entire lifecycle of digital asset transactions, including:

- Acceptance of cryptocurrency deposits;
- Management of player balances;
- Treasury management;
- Blockchain transaction monitoring;
- Cryptocurrency withdrawals;
- Wallet security;
- Digital asset custody arrangements;
- Third-party Virtual Asset Service Provider (VASP) oversight;
- Record keeping and audit requirements.

The objectives of this Policy are to:

- ensure the secure and transparent use of cryptocurrencies throughout the licensed operation;
- prevent the use of the gaming platform for money laundering, terrorist financing, fraud, sanctions evasion, or other financial crime;
- protect player assets through appropriate wallet management and security controls;
- maintain operational continuity and liquidity for player withdrawals;
- establish effective governance over treasury and digital asset management;
- support compliance with applicable legal, regulatory, and licensing requirements; and
- provide clear responsibilities for all personnel involved in cryptocurrency operations.

This Policy applies a risk-based approach to cryptocurrency operations and shall be interpreted together with all other compliance, AML/CFT, Responsible Gaming, Information Security, Incident Reporting, and Operational Risk Management policies adopted by the Operator.

Nothing contained in this Policy shall be interpreted as limiting or replacing any obligation imposed under applicable laws, regulations, licensing conditions, or directives issued by the Curaçao Gaming Authority.

2. SCOPE

This Policy applies to all cryptocurrency activities conducted by or on behalf of Satoshi Gaming Group N.V. in connection with its licensed online gaming operations.

The Policy covers all digital asset workflows throughout the player lifecycle, including but not limited to:

- cryptocurrency deposits;
- player wallet funding;
- wagering using digital assets;
- bonus and promotional transactions involving cryptocurrencies;
- cryptocurrency withdrawals;
- treasury and liquidity management;
- wallet administration;
- blockchain transaction monitoring;
- blockchain analytics;
- reconciliation of cryptocurrency balances;
- digital asset record keeping; and
- incident management involving cryptocurrency transactions.

This Policy applies to all directors, officers, employees, contractors, consultants, and third-party service providers whose responsibilities involve cryptocurrency operations or access to digital asset infrastructure.



The Operator provides gaming services exclusively to natural persons and does not offer corporate player accounts.

This Policy governs only cryptocurrency transactions directly related to licensed gaming activities.

The Operator does not:

- operate a cryptocurrency exchange;
- provide cryptocurrency brokerage services;
- provide custody services for third parties;
- facilitate peer-to-peer cryptocurrency transfers between players;
- provide wallet services unrelated to gaming activities; or
- offer investment or trading services involving digital assets.

Any activity falling outside the scope of licensed gaming operations shall be prohibited unless separately authorised under applicable law.

3. REGULATORY FRAMEWORK & GOVERNANCE

3.1 Regulatory Framework

This Policy has been established with reference to, and shall be interpreted in accordance with, the following regulatory and internal governance documents:

- The National Ordinance on Games of Chance (LOK) of Curaçao;
- Directives, guidance, and policies issued by the Curaçao Gaming Authority (CGA);
- FATF Recommendations relating to Virtual Assets and Virtual Asset Service Providers (VASPs), including Recommendation 15 and Recommendation 16 (Travel Rule), where applicable;
- The Operator's AML/CFT Policy;
- The Operator's Operations Manual;
- The Responsible Gaming Policy;
- The Information Security Policy;
- The Incident Reporting Policy; and
- Any other applicable laws, regulations, or licensing conditions governing cryptocurrency activities.

Where this Policy conflicts with applicable legislation or regulatory requirements, the applicable legal or regulatory requirement shall prevail.

3.2 Governance Principles

The Operator recognises that cryptocurrencies present unique operational, technological, financial crime, cybersecurity, and treasury risks.

Accordingly, cryptocurrency operations shall be governed under the following principles:

- accountability;
- segregation of duties;
- risk-based decision making;
- transparency;
- auditability;
- proportionality;
- operational resilience; and
- continuous monitoring.

The Operator shall ensure that cryptocurrency activities remain subject to the same standards of governance and regulatory oversight as all other licensed gaming operations.

The use of cryptocurrency shall not reduce or replace any AML/CFT, Responsible Gaming, sanctions screening, fraud prevention, or player protection obligations.

3.3 UBO

The UBO has ultimate responsibility for the governance of cryptocurrency activities conducted by the Operator.

The UBO shall:

- approve this Policy and any material amendments;
- determine the overall cryptocurrency risk appetite;
- review significant crypto-related operational risks;
- oversee treasury governance;
- ensure sufficient financial and technological resources are available;
- review material crypto-related incidents; and
- ensure that the Operator maintains compliance with applicable regulatory obligations.

The Board may delegate day-to-day responsibilities to management but retains ultimate accountability for cryptocurrency governance.

3.4 Compliance Officer

The Compliance Officer is responsible for overseeing regulatory compliance relating to cryptocurrency operations.

Responsibilities include:

- monitoring compliance with this Policy;
- ensuring alignment with AML/CFT obligations;
- monitoring regulatory developments;
- coordinating policy reviews;
- reviewing crypto-related compliance incidents;
- approving changes to cryptocurrency risk controls where required; and
- acting as the primary regulatory liaison with the Curaçao Gaming Authority regarding cryptocurrency matters.

3.5 Money Laundering Reporting Officer (MLRO)

The MLRO shall oversee all cryptocurrency-related AML/CFT activities.

Responsibilities include:

- monitoring high-risk cryptocurrency transactions;
- reviewing blockchain analytics alerts;
- assessing suspicious transaction reports;
- determining whether enhanced due diligence is required;
- reporting suspicious activities to the competent authorities where required;
- maintaining records of crypto-related AML investigations; and
- ensuring appropriate escalation of financial crime risks.

3.6 Finance and Treasury Department

The Finance Department is responsible for the operational management of cryptocurrency assets owned or controlled by the Operator.

Responsibilities include:

- maintaining operational liquidity;
- managing treasury wallets;
- performing wallet reconciliations;
- monitoring cryptocurrency balances;
- recording cryptocurrency transactions;
- safeguarding treasury assets;
- coordinating transfers between operational wallets and reserve wallets; and
- maintaining appropriate accounting records.

Finance personnel shall not have unilateral authority to initiate and approve significant cryptocurrency transfers.

Segregation of duties shall be maintained at all times.

3.7 Information Technology Department

The Information Technology Department shall maintain the technical infrastructure supporting cryptocurrency operations.

Responsibilities include:

- wallet infrastructure administration;
- private key security;
- integration with blockchain networks;
- cybersecurity controls;
- system monitoring;
- backup procedures;
- disaster recovery support;
- infrastructure maintenance; and
- implementation of technical security controls.

The IT Department shall work closely with Compliance and Finance to ensure cryptocurrency infrastructure remains secure and compliant.

3.8 Internal Audit and Independent Review

The Operator shall periodically review the effectiveness of cryptocurrency controls.

Reviews may include:

- wallet management procedures;
- treasury controls;
- blockchain monitoring processes;
- transaction reconciliation;
- access control reviews;
- cybersecurity assessments;
- compliance testing; and
- operational risk assessments.

Recommendations arising from reviews shall be documented, assigned to responsible persons, and tracked until completion.

3.9 Policy Review

This Policy shall be reviewed at least annually.

An earlier review shall be conducted whenever there is:

- a material regulatory change;
- a significant operational change;
- implementation of new cryptocurrency products;
- onboarding of new blockchain networks;
- implementation of new wallet technology;
- material cybersecurity incidents;
- significant financial crime events; or
- any other circumstance that may materially affect cryptocurrency risk.

All amendments shall be documented, version controlled, and approved in accordance with the Operator's governance procedures.

3.10 Training and Awareness

Employees whose responsibilities involve cryptocurrency operations shall receive appropriate training before being granted operational responsibilities.

Training shall include, where applicable:

- cryptocurrency fundamentals;
- blockchain technology;
- wallet security;
- blockchain analytics;
- sanctions compliance;
- AML/CFT obligations;
- fraud indicators;
- treasury procedures;
- incident reporting; and
- cybersecurity awareness.

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

4. BUSINESS MODEL & CRYPTOCURRENCY PRINCIPLES

4.1 Business Model

Satoshi Gaming Group N.V. operates a Business-to-Consumer (B2C) online gaming platform under a gaming licence issued by the Curaçao Gaming Authority.

The Operator provides online gaming services exclusively to natural persons and accepts cryptocurrency as the sole method of player deposits and withdrawals.

The Operator currently offers products including:

- Online Casino;
- Live Casino;
- Sports Betting;
- Crash Games; and
- Other approved Games of Chance.

No corporate, business, partnership, trust, or other legal entity is permitted to register or maintain a player account.

The Operator does not accept fiat currency deposits or process fiat currency withdrawals as part of its licensed gaming operations.

4.2 Cryptocurrency-Only Operations

The Operator has adopted a cryptocurrency-only operating model.

All player financial transactions are conducted using supported digital assets recorded on public blockchain networks.

Player balances are maintained in the cryptocurrency deposited by the player or another supported cryptocurrency where permitted under the Operator's Terms and Conditions and applicable internal controls.

The Operator shall maintain adequate operational liquidity to ensure timely processing of eligible player withdrawals.

The Operator continuously evaluates supported blockchain networks and digital assets to ensure operational stability, security, liquidity, and regulatory compliance.

4.3 The Operator is Not a Financial Institution

The Operator provides online gaming services only.

The Operator is not a bank, payment institution, electronic money institution, cryptocurrency exchange, broker, investment platform, or Virtual Asset Service Provider ("VASP").

Accordingly, the Operator does not provide financial services to players and shall not:

- exchange one cryptocurrency for another on behalf of players;
- exchange cryptocurrency into fiat currency on behalf of players;
- offer investment, trading, or speculative services;
- provide cryptocurrency brokerage;
- provide custodial wallet services unrelated to gaming;
- facilitate peer-to-peer cryptocurrency transfers between players;

- hold digital assets for purposes unrelated to licensed gaming activities; or
- provide remittance or payment services.

Where cryptocurrency conversion is operationally necessary, such conversion shall be performed only through appropriately regulated or otherwise suitably supervised third-party service providers engaged by the Operator for its own treasury or operational purposes and not as a service provided to players.

4.4 Cryptocurrency Principles

The Operator manages cryptocurrency activities in accordance with the following principles:

Security

Digital assets shall be protected through appropriate technical, organisational, and operational security measures.

Transparency

All cryptocurrency transactions shall be fully traceable and supported by sufficient records to facilitate reconciliation, regulatory reporting, and independent audit.

Risk-Based Control

All cryptocurrency deposits, withdrawals, wallet addresses, blockchain transactions, and counterparties shall be subject to risk-based assessment.

Higher-risk activities shall receive enhanced monitoring and additional approval where appropriate.

Player Protection

The Operator shall ensure that cryptocurrency processing supports player protection objectives, including safeguarding player funds, preventing fraud, supporting responsible gaming measures, and maintaining fair access to withdrawals.

Regulatory Compliance

Cryptocurrency operations shall comply with all applicable legal, regulatory, licensing, AML/CFT, sanctions, and Responsible Gaming obligations.



The use of cryptocurrency shall not reduce or replace any regulatory obligation applicable to the Operator.

4.5 Use of Third-Party Service Providers

The Operator may engage third-party providers to support cryptocurrency operations, including payment processors, custodial service providers, blockchain analytics providers, infrastructure providers, and Virtual Asset Service Providers (VASPs).

Prior to engagement, appropriate due diligence shall be conducted to assess:

- regulatory status;
- AML/CFT controls;
- sanctions compliance;
- cybersecurity capability;
- operational resilience;
- financial stability;
- reputation; and
- technical capability.

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

The Operator remains fully accountable for compliance with all applicable legal, regulatory, and licensing obligations.

4.6 Player Communications

The Operator shall clearly communicate to players that cryptocurrency transactions are irreversible once confirmed on the relevant blockchain network.

Players remain solely responsible for:

- selecting the correct blockchain network;
- providing accurate wallet addresses;
- maintaining control of their own wallets;
- protecting their private keys and authentication credentials; and
- ensuring compliance with applicable laws in their jurisdiction.

The Operator shall not be liable for losses arising from player errors, including but not limited to incorrect wallet addresses, unsupported blockchain networks, or transactions initiated to wallets not controlled by the intended recipient.

4.7 Changes to Supported Cryptocurrencies

The Operator reserves the right to add, suspend, or discontinue support for any cryptocurrency or blockchain network where necessary to protect players, maintain operational resilience, comply with legal or regulatory requirements, or mitigate financial crime risks.

Before introducing support for a new cryptocurrency or blockchain network, the Operator shall conduct a documented risk assessment considering, at a minimum:

- blockchain transparency;
- transaction traceability;
- market liquidity;
- price volatility;
- network stability;
- cybersecurity considerations;
- blockchain analytics coverage;
- sanctions exposure;
- AML/CFT risks; and
- operational feasibility.

All approvals relating to supported cryptocurrencies shall be documented and retained for audit purposes.

5. ACCEPTED, RESTRICTED AND PROHIBITED DIGITAL ASSETS

5.1 General Principles

The Operator shall only accept cryptocurrencies that have been formally approved through its internal Digital Asset Risk Assessment process.

The acceptance of any cryptocurrency shall be based on a documented assessment of operational, technological, financial crime, cybersecurity, legal, regulatory, and liquidity risks.

The Operator shall not support any cryptocurrency solely based on market popularity or player demand.

The Compliance Officer, Finance Department, and Information Technology Department shall jointly assess all proposed digital assets prior to implementation.

5.2 Supported Digital Assets

The Operator currently supports a limited number of cryptocurrencies that satisfy the Operator's operational and compliance requirements.

Examples of supported digital assets may include:

- Bitcoin (BTC)
- Ethereum (ETH)

The list of supported assets may be amended from time to time following completion of the Digital Asset Risk Assessment and approval by senior management.

The current list of supported cryptocurrencies shall be maintained separately by the Operations Team and published on the Operator's gaming platform.

5.3 Digital Asset Approval Criteria

Before a cryptocurrency is accepted, the following factors shall be considered:

Regulatory Considerations

The asset shall not be prohibited by applicable laws or regulatory requirements applicable to the Operator.

Where regulatory uncertainty exists, additional legal or compliance review shall be conducted.

Blockchain Transparency

Preference shall be given to blockchain networks that provide transparent and publicly verifiable transaction histories.

The Operator shall favour cryptocurrencies that support effective blockchain analytics and transaction tracing.

AML/CFT Risk

The cryptocurrency shall be capable of supporting effective:

- wallet screening;
- sanctions screening;
- transaction monitoring;
- source of funds assessment;
- blockchain investigation; and
- suspicious transaction analysis.

Cybersecurity

The blockchain network shall demonstrate an acceptable level of security, resilience, decentralisation, and resistance to known attacks.

Consideration shall include:

- network stability;
- historical security incidents;
- consensus mechanism;
- blockchain maturity; and
- software support.

Liquidity

The cryptocurrency shall maintain sufficient market liquidity to support operational treasury activities and timely player withdrawals.

Operational Compatibility

The Information Technology Department shall confirm that the asset can be safely integrated into the Operator's infrastructure.

Consideration shall include:

- wallet compatibility;
- blockchain node reliability;
- transaction confirmation times;
- network fees;
- API stability; and
- disaster recovery capability.

5.4 Stablecoin Assessment

Where stablecoins are accepted, additional risks shall be considered, including:

- reserve transparency;
- issuer governance;
- redemption mechanisms;
- regulatory status of the issuer;
- de-pegging risk;
- concentration risk;
- blockchain network availability; and

- historical operational performance.

The Operator shall continuously monitor material developments affecting supported stablecoins.

Where a stablecoin presents unacceptable operational, regulatory, or financial risks, the Operator may suspend deposits, withdrawals, or both until such risks have been adequately mitigated.

5.5 Restricted Digital Assets

Certain cryptocurrencies may be classified as Restricted Assets.

Restricted Assets may only be supported following enhanced review and documented approval.

Factors that may result in a Restricted classification include:

- elevated market volatility;
- limited blockchain analytics capability;
- low market liquidity;
- newly launched blockchain networks;
- significant cybersecurity concerns;
- uncertain regulatory treatment; or
- operational limitations.

Additional monitoring and transaction controls may be applied to Restricted Assets.

5.6 Prohibited Digital Assets

The Operator shall not knowingly accept cryptocurrencies or digital assets that present an unacceptable level of financial crime, regulatory, or operational risk.

Without limitation, the following categories shall generally be prohibited:

- privacy-enhanced cryptocurrencies that significantly impede transaction tracing;
- digital assets primarily designed to obscure transaction origin or destination;
- sanctioned digital assets;
- assets associated with ransomware activities;
- assets linked to terrorist financing;
- assets connected with darknet marketplaces;
- assets identified as stolen or fraudulently obtained;
- assets subject to regulatory prohibition; or
- any cryptocurrency that cannot be effectively monitored using the Operator's blockchain analytics capabilities.

The Operator reserves the right to reject any deposit or refuse any withdrawal involving such assets.

5.7 Unsupported Blockchain Networks

Where a supported cryptocurrency exists on multiple blockchain networks, the Operator shall only accept deposits made through officially supported networks.

Deposits sent through unsupported blockchain networks may be unrecoverable.

The list of supported blockchain networks shall be published on the Operator's gaming platform and reviewed periodically.

5.8 Periodic Review of Supported Assets

All supported cryptocurrencies and blockchain networks shall be reviewed periodically to ensure they remain appropriate for the Operator's licensed activities.

The review shall consider:

- regulatory developments;
- blockchain security;
- liquidity;
- transaction monitoring capability;
- sanctions exposure;
- operational performance;
- cybersecurity threats;
- player usage;
- treasury requirements; and
- business continuity.

Where a material risk is identified, the Operator may suspend or discontinue support for the relevant cryptocurrency or blockchain network.

5.9 Emergency Suspension

The Operator may immediately suspend the acceptance or withdrawal of any cryptocurrency where necessary to protect players or the integrity of the gaming operation.

Examples include:

- blockchain compromise;
- significant network instability;

- prolonged blockchain outage;
- critical software vulnerabilities;
- sanctions developments;
- blockchain forks creating operational uncertainty;
- credible cybersecurity threats; or
- directions issued by the Curaçao Gaming Authority or other competent authorities.

Emergency decisions shall be documented and reviewed as soon as reasonably practicable.

6. BLOCKCHAIN ANALYTICS & TRANSACTION MONITORING

6.1 Purpose

The Operator shall implement appropriate blockchain analytics and transaction monitoring controls to identify, assess, and mitigate financial crime risks associated with cryptocurrency transactions.

Blockchain analytics form an integral part of the Operator's Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) framework and support compliance with applicable legal, regulatory, and licensing obligations.

The objectives of blockchain transaction monitoring are to:

- identify high-risk cryptocurrency wallets;
- detect suspicious transaction patterns;
- support sanctions compliance;
- assist Source of Funds (SOF) assessments;
- identify links to illicit activities;
- protect the Operator from financial crime exposure; and
- support regulatory reporting where required.

6.2 Risk-Based Monitoring

All cryptocurrency transactions shall be subject to a risk-based monitoring framework.

Monitoring measures shall be proportionate to the level of risk presented by the player, wallet address, transaction characteristics, blockchain network, and any other relevant risk indicators.

Higher-risk transactions shall receive enhanced review before funds are credited or withdrawals are approved.

6.3 Wallet Screening

The Operator shall screen cryptocurrency wallet addresses using appropriate blockchain analytics solutions before processing deposits or withdrawals where operationally feasible.

Wallet screening may identify potential links to:

- sanctioned persons or entities;
- terrorist financing;
- ransomware activities;
- darknet marketplaces;
- fraud;
- stolen assets;
- scams;
- phishing activities;
- mixers or tumblers;
- illicit marketplaces; or
- other criminal activity.

Where elevated risks are identified, additional due diligence shall be performed.

6.4 Transaction Risk Assessment

Each cryptocurrency transaction may be assessed using multiple risk indicators, including:

- blockchain risk profile;
- wallet risk score;
- transaction amount;
- transaction frequency;
- transaction velocity;
- historical player behaviour;
- jurisdictional exposure;
- source wallet characteristics;
- destination wallet characteristics;
- sanctions exposure; and
- other relevant intelligence.

No single indicator shall automatically determine whether a transaction is suspicious.

The Operator shall consider the overall circumstances before making a risk determination.

6.5 High-Risk Indicators

Examples of higher-risk indicators include, but are not limited to:

- transactions involving wallets associated with sanctioned persons or jurisdictions;

- transactions linked to known illicit services;
- repeated deposits from multiple unrelated wallets;
- rapid movement of funds without corresponding gaming activity;
- unusually large deposits inconsistent with the player's profile;
- multiple failed withdrawal attempts;
- significant changes in transaction behaviour;
- attempts to circumvent internal controls;
- blockchain activity indicating possible layering; or
- any activity giving rise to reasonable suspicion of money laundering, terrorist financing, fraud, or sanctions evasion.

The presence of one or more indicators shall trigger further review but shall not automatically result in account closure.

6.6 Enhanced Review

Where elevated cryptocurrency risk is identified, the Operator may apply Enhanced Due Diligence (EDD).

EDD measures may include:

- requesting additional identification documents;
- requesting Source of Funds (SOF) information;
- obtaining Source of Wealth (SOW) information where appropriate;
- requesting explanations regarding cryptocurrency activity;
- conducting additional blockchain analysis;
- reviewing previous transaction history;
- temporary suspension of withdrawals pending review; or
- escalation to the MLRO.

The scope of EDD shall be proportionate to the identified risk.

6.7 Sanctions Compliance

The Operator shall implement controls designed to prevent transactions involving sanctioned persons, sanctioned entities, or sanctioned cryptocurrency wallets.

Sanctions screening shall be conducted in accordance with the Operator's Sanctions Policy.

Where sanctions concerns are identified, transactions may be suspended while further investigation is undertaken.

Where required by law, assets may be frozen and reports submitted to the competent authorities.

6.8 Ongoing Monitoring

Cryptocurrency risk monitoring is an ongoing process.

Player activity shall be periodically reviewed throughout the business relationship.

Monitoring may include:

- cumulative transaction volumes;
- changes in wallet usage;
- gaming behaviour;
- withdrawal patterns;
- repeated deposits;
- blockchain exposure;
- changes in player risk profile; and
- new intelligence received from blockchain analytics providers.

Where a player's overall risk profile changes materially, the Operator may update the player's risk classification and apply additional monitoring or due diligence measures.

6.9 Suspicious Activity Escalation

Employees identifying unusual cryptocurrency activity shall immediately report the matter to the Compliance Department or the MLRO.

No employee shall inform the player that an internal review or suspicious activity assessment is being conducted.

All investigations shall remain confidential and be handled in accordance with the Operator's AML/CFT Policy.

Where appropriate, Suspicious Activity Reports (SARs) or equivalent regulatory reports shall be submitted to the competent authorities.

6.10 Record Keeping

The Operator shall maintain adequate records relating to blockchain monitoring activities.

Records may include:

- blockchain transaction hashes (TxIDs);
- wallet screening results;
- blockchain analytics reports;
- sanctions screening results;

- transaction risk assessments;
- enhanced due diligence records;
- internal investigation notes;
- decisions made during reviews; and
- supporting evidence relied upon.

Such records shall be retained in accordance with the Operator's Record Retention Policy and made available to the Curaçao Gaming Authority upon lawful request.

6.11 Continuous Improvement

The Operator shall periodically evaluate the effectiveness of its blockchain analytics and transaction monitoring framework.

This evaluation may consider:

- emerging financial crime typologies;
- new blockchain technologies;
- regulatory developments;
- cybersecurity threats;
- performance of blockchain analytics providers;
- internal incident reports; and
- independent audit findings.

Where deficiencies are identified, corrective actions shall be implemented in a timely manner to ensure that monitoring controls remain effective and proportionate to the Operator's risk profile.

7. CRYPTOCURRENCY DEPOSIT CONTROLS

7.1 Purpose

The Operator shall implement appropriate controls to ensure that cryptocurrency deposits are processed securely, accurately, and in compliance with applicable legal, regulatory, AML/CFT, and operational requirements.

Cryptocurrency deposits shall only be accepted for the purpose of funding a player's gaming account.

The Operator shall not accept cryptocurrency deposits for investment, custody, payment, remittance, or any purpose unrelated to licensed gaming activities.

7.2 Supported Deposit Assets

Players may only deposit cryptocurrencies that are:

- officially supported by the Operator;
- transferred via supported blockchain networks; and
- deposited to wallet addresses generated or designated by the Operator.

The current list of supported cryptocurrencies and blockchain networks shall be published on the Operator's gaming platform.

Deposits made using unsupported cryptocurrencies or unsupported blockchain networks may not be recoverable.

7.3 Player Wallet Addresses

Each player shall be provided with a designated cryptocurrency deposit address or another approved deposit mechanism supported by the Operator.

Deposit addresses shall be generated and managed using secure wallet infrastructure.

The Operator shall implement appropriate controls to minimise address reuse where operationally practicable.

Players are responsible for ensuring that deposits are made to the correct wallet address and through the correct blockchain network.

7.4 Blockchain Confirmation Requirements

Cryptocurrency deposits shall not be credited immediately upon broadcast to the blockchain.

Deposits shall only be credited after the required number of blockchain confirmations has been received.

Confirmation requirements shall be determined by the Operator based on:

- blockchain security;
- network stability;
- historical reorganisation risk;
- operational considerations; and
- asset-specific characteristics.

The Operator reserves the right to increase confirmation requirements where elevated blockchain risks are identified.

7.5 Deposit Screening

Before crediting player funds, the Operator may perform appropriate compliance and risk assessments.

These assessments may include:

- wallet screening;
- blockchain analytics;
- sanctions screening;
- fraud detection;
- transaction pattern analysis;
- player risk assessment; and
- other AML/CFT controls.

Where elevated risk is identified, deposits may be subject to additional review before funds become available for gaming.

7.6 High-Risk Deposits

Deposits presenting elevated financial crime, fraud, cybersecurity, or regulatory risks shall be escalated for review.

Examples include:

- unusually large deposits;
- deposits inconsistent with previous player behaviour;
- deposits associated with high-risk wallet addresses;
- transactions involving sanctioned jurisdictions;
- repeated deposits from multiple unrelated wallets;
- blockchain activity indicating potential layering; or
- other suspicious circumstances identified through risk monitoring.

Additional due diligence may be required before such deposits are accepted.

7.7 Incorrect or Unsupported Deposits

Where a player sends cryptocurrency:

- using an unsupported blockchain network;
- using an unsupported digital asset;
- to an incorrect wallet address; or
- contrary to published deposit instructions,

the Operator shall use reasonable efforts to assess whether recovery is technically feasible.

The Operator does not guarantee recovery of incorrectly transmitted digital assets.

Any recovery process may:

- require additional verification;
- incur administrative or blockchain-related costs;
- take an extended period of time; or
- be technically impossible.

7.8 Deposit Limits

The Operator may establish risk-based deposit limits designed to support:

- responsible gaming;
- AML/CFT compliance;
- fraud prevention;
- operational risk management; and
- player protection.

Deposit limits may vary according to:

- player verification status;
- risk classification;
- source of funds assessments;
- account history; and
- regulatory requirements.

7.9 Source of Funds

Where appropriate, the Operator may require players to provide evidence regarding the legitimate source of cryptocurrency deposits.

Requests may include information relating to:

- employment income;
- business activities;
- investment proceeds;
- mining activities;
- cryptocurrency trading history;
- inheritance;
- asset sales; or
- other lawful sources of wealth or funds.

Failure to provide satisfactory information may result in restrictions being applied to the player account.

7.10 Deposit Reconciliation

All cryptocurrency deposits shall be reconciled against:

- blockchain transaction records;
- wallet balances;
- player account balances; and
- accounting records.

Reconciliations shall be performed on a regular basis to ensure the completeness and accuracy of financial records.

Any discrepancies shall be investigated promptly and documented.

7.11 Deposit Records

The Operator shall maintain accurate records relating to cryptocurrency deposits.

Records may include:

- player identification;
- wallet address;
- blockchain network;
- cryptocurrency type;
- transaction hash (TxID);
- deposit amount;
- blockchain confirmation details;
- timestamp;
- wallet screening results;
- risk assessment outcome; and
- any additional compliance documentation.

Such records shall be retained in accordance with the Operator's Record Retention Policy and made available to the Curaçao Gaming Authority upon lawful request.

8. CRYPTOCURRENCY WITHDRAWAL CONTROLS

8.1 Purpose

The Operator shall implement appropriate controls to ensure that cryptocurrency withdrawals are processed securely, accurately, and in compliance with applicable legal, regulatory, AML/CFT, sanctions, fraud prevention, and responsible gaming requirements.

Withdrawal controls are designed to:

- safeguard player funds;
- prevent money laundering and terrorist financing;
- reduce fraud and account takeover risks;
- ensure operational integrity;
- maintain treasury liquidity; and
- comply with all applicable licensing obligations.

8.2 Withdrawal Eligibility

Before a withdrawal is processed, the Operator shall verify that:

- the player account is active;
- the player has successfully completed any required identity verification;
- the withdrawal request complies with the Operator's Terms and Conditions;
- sufficient cleared balance is available;
- no regulatory, AML/CFT, fraud, or Responsible Gaming restrictions apply; and
- there are no outstanding investigations affecting the account.

The Operator reserves the right to delay or refuse withdrawals where additional verification is reasonably required.

8.3 Destination Wallet Verification

Players are responsible for providing an accurate cryptocurrency wallet address.

Before processing a withdrawal, the Operator may verify:

- blockchain network compatibility;
- wallet address format;
- supported cryptocurrency;
- sanctions exposure;
- blockchain risk indicators; and
- other relevant compliance information.

Where the destination wallet presents an elevated level of risk, additional review may be conducted before the withdrawal is approved.

8.4 Withdrawal Risk Assessment

Each withdrawal request may be subject to a risk-based assessment considering factors including:

- player verification status;
- account age;
- transaction history;
- withdrawal amount;
- cumulative withdrawal activity;
- recent deposits;
- gaming activity;
- blockchain analytics results;
- sanctions screening results;
- fraud indicators;
- responsible gaming concerns; and
- any other relevant risk factors.

The extent of review shall be proportionate to the assessed level of risk.

8.5 Enhanced Review

The Operator may conduct Enhanced Due Diligence (EDD) prior to approving a withdrawal where elevated risks are identified.

EDD measures may include:

- requesting additional identity documentation;
- requesting Source of Funds information;
- requesting Source of Wealth information where appropriate;
- obtaining clarification regarding wallet ownership or transaction history;
- conducting enhanced blockchain analytics;
- reviewing historical account activity; and
- escalating the matter to the Compliance Officer or MLRO.

Withdrawal processing may be temporarily suspended until the review has been completed.

8.6 Manual Approval

Certain withdrawal requests shall require manual review and approval.

Examples include:

- unusually large withdrawals;

- withdrawals inconsistent with normal player behaviour;
- transactions involving higher-risk wallets;
- withdrawals following limited or no gaming activity;
- repeated withdrawal attempts after failed verification;
- withdrawals subject to regulatory review; or
- any circumstance where automated controls identify elevated risk.

The Operator shall maintain appropriate segregation of duties between personnel responsible for reviewing, approving, and executing withdrawals.

8.7 Treasury Liquidity Verification

Before a withdrawal is broadcast to the blockchain, the Finance Department shall ensure that:

- sufficient operational liquidity is available;
- treasury balances remain within approved limits;
- the withdrawal does not adversely affect operational continuity; and
- any required transfer from reserve or cold storage wallets has been completed in accordance with internal approval procedures.

Where temporary liquidity constraints arise, withdrawals may be processed in the order received, subject to operational requirements and applicable legal obligations.

8.8 Blockchain Transaction Controls

All cryptocurrency withdrawals shall be processed through secure wallet infrastructure.

Appropriate technical controls shall include, where applicable:

- multi-factor authentication;
- multi-signature or equivalent approval mechanisms;
- withdrawal authorisation controls;
- transaction validation;
- blockchain confirmation of successful broadcast;
- audit logging; and
- secure management of private keys.

Transaction hashes (TxIDs) shall be recorded following successful blockchain transmission.

8.9 Rejected or Suspended Withdrawals

The Operator may reject, suspend, or delay a withdrawal where:

- the player has not completed required verification;
- AML/CFT concerns exist;
- sanctions concerns exist;
- fraud is suspected;
- responsible gaming interventions are required;
- the destination wallet presents unacceptable risk;
- legal or regulatory restrictions apply; or
- technical issues prevent secure processing.

Where appropriate, the Operator shall inform the player of any additional information required to progress the withdrawal, except where doing so would be prohibited by law or could constitute unlawful tipping-off.

8.10 Withdrawal Records

The Operator shall maintain complete records relating to all cryptocurrency withdrawals.

Records may include:

- player identification;
- destination wallet address;
- cryptocurrency type;
- blockchain network;
- withdrawal amount;
- transaction hash (TxID);
- timestamp;
- approval records;
- blockchain analytics results;
- sanctions screening results;
- risk assessment records;
- enhanced due diligence records (where applicable); and
- any supporting correspondence or documentation.

Records shall be retained in accordance with the Operator's Record Retention Policy and made available to the Curaçao Gaming Authority upon lawful request.

8.11 Withdrawal Monitoring

The Operator shall periodically review withdrawal activity to identify unusual patterns or emerging risks.

Monitoring may include:

- withdrawal frequency;

- cumulative withdrawal values;
- changes in destination wallets;
- withdrawal-to-deposit ratios;
- gaming activity prior to withdrawal;
- links to high-risk blockchain activity; and
- other indicators of financial crime or fraud.

Where necessary, the Operator shall implement additional controls or enhanced monitoring to mitigate identified risks.

9. TREASURY MANAGEMENT

9.1 Purpose

The purpose of the Treasury Management framework is to ensure that the Operator maintains sufficient liquidity, security, operational resilience, and financial integrity in managing cryptocurrency assets used in its licensed gaming operations.

Treasury Management is designed to:

- safeguard player funds;
- maintain sufficient liquidity for player withdrawals;
- minimise operational and cybersecurity risks;
- protect corporate digital assets;
- support business continuity;
- facilitate accurate financial reporting; and
- ensure compliance with applicable legal, regulatory, and licensing obligations.

Treasury activities shall be conducted prudently and solely for operational purposes. The Operator shall not use player funds for proprietary cryptocurrency trading, speculative investment, lending, staking, yield farming, or other high-risk investment activities.

9.2 Segregation of Funds

The Operator shall maintain clear segregation between:

- player funds;
- operational funds;
- treasury reserve assets; and
- corporate working capital.

Player balances shall not be intentionally used to finance operating expenses or speculative activities.

Internal accounting records shall accurately distinguish between player liabilities and assets belonging to the Operator.

9.3 Treasury Wallet Structure

To reduce operational and cybersecurity risks, the Operator shall maintain separate wallet categories according to operational purpose.

These may include:

Deposit Wallets

Used solely to receive player deposits.

Operational (Hot) Wallets

Used to process routine player withdrawals and day-to-day operational requirements.

Only the amount reasonably required for anticipated operational activities shall be maintained in Hot Wallets.

Treasury Wallets

Used to hold operational liquidity exceeding normal daily requirements.

Treasury Wallets shall not normally interact directly with player accounts.

Cold Storage Wallets

Used for long-term storage of the majority of corporate cryptocurrency holdings.

Cold Wallets shall remain offline or otherwise protected using enhanced security controls whenever operationally practicable.

The Operator may implement additional wallet categories where appropriate to support operational efficiency or security.

9.4 Liquidity Management

The Finance Department shall continuously monitor operational liquidity to ensure that sufficient cryptocurrency is available to satisfy expected withdrawal requests.

Liquidity assessments shall consider:

- historical withdrawal activity;

- expected player demand;
- business growth;
- promotional campaigns;
- market conditions;
- blockchain network congestion;
- settlement timeframes; and
- operational contingency requirements.

Where necessary, assets may be transferred between approved treasury wallets to maintain appropriate operational liquidity.

9.5 Daily Treasury Operations

Treasury balances shall be reviewed on each business day.

Routine treasury activities may include:

- reconciliation of wallet balances;
- transfer of excess funds from Deposit Wallets to Treasury Wallets;
- replenishment of Operational Wallets;
- review of pending withdrawals;
- review of blockchain transaction status;
- monitoring of network fees;
- monitoring of stablecoin exposure; and
- verification of treasury records.

All treasury movements shall be recorded and supported by appropriate audit trails.

9.6 Stablecoin Management

Where stablecoins are used within the Operator's business, the Finance Department shall monitor risks associated with those assets.

Risk factors include:

- issuer stability;
- reserve transparency;
- regulatory developments;
- market liquidity;
- blockchain network stability;
- de-pegging events;
- concentration risk; and
- operational availability.

Where a supported stablecoin presents material operational or financial risks, the Operator may suspend acceptance of that stablecoin until the identified risks have been adequately addressed.

9.7 Treasury Exposure Limits

The Operator shall establish internal limits designed to reduce concentration risk.

The Finance Department shall monitor exposure to:

- individual cryptocurrencies;
- individual blockchain networks;
- individual wallet infrastructure;
- individual third-party service providers; and
- operational liquidity reserves.

Where internal limits are exceeded, appropriate corrective action shall be taken as soon as reasonably practicable.

Specific exposure thresholds may be maintained in separate internal treasury procedures and may be adjusted from time to time according to business needs.

9.8 Treasury Reconciliation

Treasury balances shall be reconciled regularly.

Reconciliation shall include comparison of:

- blockchain balances;
- wallet balances;
- player liability records;
- accounting records;
- treasury records; and
- financial reporting data.

Any discrepancies shall be investigated promptly.

Material discrepancies shall be reported to senior management and, where appropriate, the Compliance Officer.

9.9 Emergency Liquidity Management

The Operator shall maintain procedures to address temporary liquidity shortages or operational disruptions.

Contingency measures may include:

- transferring assets from Treasury Wallets to Operational Wallets;
- transferring assets from Cold Storage to Treasury Wallets;
- adjusting withdrawal processing priorities based on operational requirements;
- activating disaster recovery procedures; or
- implementing other approved contingency measures.

Emergency treasury actions shall be documented and subject to appropriate post-incident review.

9.10 Treasury Security

Treasury assets shall be protected using appropriate technical and organisational controls.

Such controls may include:

- segregation of duties;
- multi-factor authentication;
- multi-signature or equivalent approval mechanisms;
- role-based access controls;
- transaction approval workflows;
- secure private key management;
- audit logging; and
- periodic access reviews.

No single individual shall have unrestricted authority to initiate, approve, and execute significant treasury transfers without appropriate oversight, except where emergency procedures approved by senior management apply.

9.11 Treasury Reporting

The Finance Department shall prepare periodic treasury reports for senior management.

Reports may include:

- wallet balances;
- liquidity position;
- significant treasury transfers;
- stablecoin exposure;
- concentration risks;
- reconciliation results;
- operational incidents;
- blockchain fee trends; and

- material treasury risks.

Treasury reporting shall support effective governance and management oversight.

9.12 Continuous Review

Treasury Management procedures shall be reviewed periodically to ensure that they remain appropriate for the Operator's business model, transaction volumes, supported cryptocurrencies, and regulatory obligations.

Changes to treasury procedures shall be documented, approved, and communicated to relevant personnel before implementation.

10. WALLET MANAGEMENT & PRIVATE KEY SECURITY

10.1 Purpose

The Operator shall implement appropriate governance, operational procedures, and technical controls to protect cryptocurrency wallets and private keys used in connection with its licensed gaming operations.

Wallet management controls are designed to:

- safeguard digital assets;
- minimise cybersecurity risks;
- prevent unauthorised transactions;
- ensure operational resilience;
- maintain business continuity; and
- support compliance with applicable legal and regulatory requirements.

10.2 Wallet Classification

Cryptocurrency wallets shall be classified according to their operational purpose.

Deposit Wallets

Deposit Wallets are used solely to receive cryptocurrency deposits from players.

These wallets shall not normally be used to store significant operational balances.

Operational (Hot) Wallets



Operational Wallets are connected to systems supporting routine player withdrawals.

Only sufficient cryptocurrency required for normal operational activities shall be maintained within Hot Wallets.

Balances shall be reviewed regularly and replenished from Treasury Wallets when necessary.

Treasury Wallets

Treasury Wallets are used to hold operational reserves that exceed normal daily withdrawal requirements.

Access to Treasury Wallets shall be subject to enhanced approval controls.

Cold Storage Wallets

Cold Storage Wallets are intended for the long-term safeguarding of corporate cryptocurrency reserves.

Where operationally practicable, Cold Wallets shall remain isolated from internet-connected systems.

Transfers from Cold Storage shall only occur following appropriate authorisation procedures.

10.3 Wallet Ownership and Control

All wallets used for licensed gaming operations shall be owned or controlled by the Operator or by appropriately authorised third-party service providers acting on behalf of the Operator.

The Operator shall maintain an internal register identifying:

- wallet purpose;
- supported cryptocurrency;
- blockchain network;
- responsible department;
- operational status; and
- date of creation or retirement.

10.4 Private Key Protection

Private keys shall be protected throughout their lifecycle.

Appropriate security measures may include:

- encryption;
- secure generation procedures;
- restricted access;
- secure storage;
- key fragmentation or equivalent controls;
- hardware security devices where appropriate; and
- secure backup procedures.

Private keys shall never be disclosed to unauthorised persons.

10.5 Access Management

Access to wallet infrastructure shall be granted strictly on the basis of business necessity.

The Operator shall implement role-based access controls to ensure that personnel receive only the minimum level of access necessary to perform their duties.

Access rights shall be:

- formally approved;
- documented;
- periodically reviewed; and
- removed immediately when no longer required.

10.6 Segregation of Duties

The Operator shall maintain segregation of duties within wallet management processes.

Where practicable, responsibility for the following activities shall be separated:

- wallet administration;
- transaction initiation;
- transaction approval;
- transaction execution;
- reconciliation; and
- compliance review.

No individual shall have unrestricted authority to complete an entire high-value cryptocurrency transfer independently under normal operating conditions.

10.7 Transaction Authorisation

Significant cryptocurrency transfers shall be subject to appropriate approval procedures.

Authorisation controls may include:

- multi-signature approval;
- multi-party approval;
- delegated approval authority;
- transaction limits;
- treasury approval workflows; or
- other equivalent security mechanisms.

The approval process shall be proportionate to the value and risk associated with the transaction.

10.8 Wallet Monitoring

Wallet infrastructure shall be monitored on an ongoing basis.

Monitoring activities may include:

- wallet availability;
- blockchain connectivity;
- unusual transaction activity;
- failed transaction attempts;
- abnormal access attempts;
- system alerts;
- balance monitoring; and
- security event monitoring.

Material security events shall be escalated in accordance with the Operator's Incident Response procedures.

10.9 Wallet Backup and Recovery

The Operator shall maintain appropriate procedures for wallet recovery in the event of technical failure or other operational disruption.

Recovery arrangements shall ensure that:

- authorised personnel can restore access where necessary;
- recovery procedures are periodically tested;
- backup materials are securely protected; and
- recovery documentation remains current.

Backup materials shall be protected to the same standard as production private keys.

10.10 Wallet Lifecycle Management

The Operator shall maintain procedures governing the complete lifecycle of cryptocurrency wallets.

This includes:

- wallet creation;
- operational activation;
- configuration management;
- periodic review;
- retirement of obsolete wallets; and
- secure destruction of wallet credentials where applicable.

Inactive wallets shall not remain operational unless there is a legitimate business requirement.

10.11 Security Reviews

Wallet security controls shall be reviewed periodically.

Reviews may include:

- access reviews;
- key management reviews;
- penetration testing;
- vulnerability assessments;
- configuration reviews;
- transaction approval testing;
- reconciliation testing; and
- independent security assessments.

Any weaknesses identified shall be documented, risk assessed, and remediated within an appropriate timeframe.

10.12 Lost or Compromised Wallets

Where there is reason to believe that a wallet or private key has been lost, compromised, or exposed to unauthorised access, the Operator shall immediately activate its Incident Response procedures.

Appropriate actions may include:

- suspension of affected wallet activity;
- transfer of assets to secure wallets where feasible;

- investigation of the incident;
- notification of senior management;
- engagement of relevant service providers;
- preservation of audit evidence; and
- notification to the Curaçao Gaming Authority or other competent authorities where required by law or licence conditions.

All such incidents shall be documented, investigated, and reviewed to identify opportunities for improving security controls.

10.13 Continuous Improvement

The Operator shall periodically evaluate developments in cryptocurrency security technologies and industry best practices.

Where appropriate, the Operator may implement enhanced security measures, including new wallet technologies, authentication methods, cryptographic controls, or operational procedures to further strengthen the protection of digital assets.

11. THIRD-PARTY SERVICE PROVIDERS & VIRTUAL ASSET SERVICE PROVIDERS (VASPs)

11.1 Purpose

The Operator may engage third-party service providers to support cryptocurrency-related activities where such engagement enhances operational efficiency, security, compliance, or business continuity.

The Operator remains fully responsible for compliance with all applicable legal, regulatory, and licensing obligations, irrespective of whether cryptocurrency-related activities are performed internally or by external service providers.

Appropriate governance and oversight shall therefore be maintained throughout the entire lifecycle of every third-party relationship.

11.2 Scope

Third-party providers may include, but are not limited to:

- Virtual Asset Service Providers (VASPs);
- cryptocurrency payment processors;
- blockchain analytics providers;

- wallet infrastructure providers;
- digital asset custodians;
- cloud infrastructure providers;
- cybersecurity service providers;
- node infrastructure providers;
- treasury support providers; and
- other technology vendors supporting cryptocurrency operations.

11.3 Due Diligence

Before engaging a third-party service provider, the Operator shall perform documented due diligence appropriate to the level of risk presented.

The assessment may include:

- legal status;
- ownership structure;
- licensing or regulatory status where applicable;
- financial stability;
- operational capability;
- information security controls;
- AML/CFT framework;
- sanctions compliance;
- business reputation;
- incident history;
- business continuity capability; and
- technical compatibility.

The depth of due diligence shall be proportionate to the importance of the outsourced service.

11.4 Risk Assessment

Prior to onboarding a third-party provider, the Operator shall perform a documented risk assessment considering, where relevant:

- operational risk;
- financial crime risk;
- cybersecurity risk;
- concentration risk;
- jurisdictional risk;
- data protection risk;
- service continuity;
- regulatory risk; and

- dependency on critical infrastructure.

Appropriate mitigating controls shall be implemented before services commence.

11.5 Contractual Requirements

All material third-party relationships shall be governed by written agreements.

Such agreements should address, where appropriate:

- scope of services;
- service availability;
- security obligations;
- confidentiality;
- regulatory cooperation;
- audit rights;
- incident notification;
- subcontracting;
- business continuity;
- termination rights;
- record retention; and
- compliance with applicable laws.

The Operator shall retain copies of executed agreements in accordance with its document retention procedures.

11.6 Ongoing Monitoring

Third-party providers shall be subject to ongoing monitoring throughout the duration of the relationship.

Monitoring activities may include:

- periodic performance reviews;
- security reviews;
- service level monitoring;
- regulatory status monitoring;
- review of material incidents;
- financial condition monitoring;
- review of audit reports where available;
- penetration testing reports where applicable;
- business continuity testing; and
- annual risk reassessment.

Where material deficiencies are identified, corrective action shall be requested within an appropriate timeframe.

11.7 Information Security

Third-party providers handling cryptocurrency-related services shall maintain information security controls appropriate to the sensitivity of the services provided.

Where appropriate, the Operator may assess whether providers maintain recognised security standards, certifications, or equivalent internal control frameworks.

Access to Operator systems and data shall be limited to the minimum necessary to perform contracted services.

11.8 Business Continuity

Critical service providers shall maintain appropriate business continuity and disaster recovery arrangements.

Where practical, the Operator shall evaluate:

- redundancy arrangements;
- backup procedures;
- recovery objectives;
- operational resilience;
- cyber incident response capability; and
- service restoration procedures.

The Operator shall maintain contingency arrangements for critical outsourced services where feasible.

11.9 FATF Travel Rule

Where the Operator engages with a regulated Virtual Asset Service Provider (VASP) in connection with cryptocurrency transfers, the Operator shall cooperate with the VASP to facilitate compliance with applicable Travel Rule requirements where such requirements apply under relevant law.

The Operator recognises that Travel Rule obligations primarily apply to regulated VASPs and that the applicability of such obligations depends upon the legal status of the parties involved, the nature of the transaction, and the jurisdictions concerned.

Accordingly, where cryptocurrency transfers are processed through or involve regulated VASPs, the Operator shall:

- provide information reasonably required by the VASP to support regulatory compliance;
- cooperate with lawful information requests;
- maintain appropriate transaction records;
- support AML/CFT investigations where required;
- comply with applicable sanctions obligations; and
- implement any additional controls required by applicable law.

Nothing in this Policy shall require the Operator to collect or transmit information beyond that required by applicable legal or regulatory obligations.

11.10 Incident Management

Third-party providers shall notify the Operator without undue delay of any material incident that may affect:

- cryptocurrency security;
- wallet infrastructure;
- player assets;
- service availability;
- regulatory compliance;
- cybersecurity;
- personal data; or
- business continuity.

The Operator shall assess the impact of each incident and determine whether escalation to senior management, the Compliance Officer, the MLRO, or the Curaçao Gaming Authority is required.

11.11 Termination of Third-Party Relationships

Where a third-party provider no longer meets the Operator's operational, security, regulatory, or contractual requirements, the Operator may suspend or terminate the relationship.

Prior to termination, the Operator shall, where appropriate:

- ensure continuity of critical services;
- recover relevant operational data;
- revoke system access;
- complete reconciliation of outstanding transactions;
- securely return or destroy confidential information where applicable; and
- document the closure of the relationship.

The termination process shall minimise disruption to licensed gaming operations and protect player interests.

12. CRYPTOCURRENCY AML/CFT CONTROLS

12.1 Purpose

The Operator shall implement risk-based Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) controls specifically applicable to cryptocurrency activities conducted as part of its licensed gaming operations.

These controls supplement, and shall be read together with, the Operator's AML/CFT Policy.

Where any inconsistency exists, the requirements of the AML/CFT Policy and applicable legislation shall prevail.

The Operator shall adopt a risk-based approach when assessing cryptocurrency-related risks.

Risk assessments shall consider, where appropriate:

- customer risk;
- geographic risk;
- blockchain network risk;
- digital asset risk;
- wallet risk;
- transaction risk;
- delivery channel risk;
- sanctions exposure;
- source of funds; and
- emerging financial crime typologies.

AML/CFT controls shall be proportionate to the assessed level of risk.

12.3 Customer Due Diligence

The Operator shall conduct Customer Due Diligence (CDD) in accordance with its AML/CFT Policy.

Cryptocurrency-related information may be considered as part of the overall customer risk assessment.

CDD measures may include:

- identity verification;
- sanctions screening;
- politically exposed person (PEP) screening;
- jurisdictional assessment;
- source of funds enquiries where appropriate;
- source of wealth enquiries for higher-risk customers; and
- ongoing monitoring.

12.4 Source of Funds and Source of Wealth

Where required by the Operator's risk assessment, players may be requested to provide information regarding the legitimate origin of cryptocurrency used within the gaming platform.

Examples of acceptable supporting information may include:

- employment income;
- business income;
- investment proceeds;
- cryptocurrency trading history;
- mining income;
- inheritance;
- sale of assets; or
- other lawful sources.

The extent of documentation requested shall be proportionate to the identified risk.

12.5 Wallet Risk Assessment

The Operator shall assess cryptocurrency wallet addresses using appropriate blockchain analytics tools where operationally feasible.

Wallet assessments may consider:

- sanctions exposure;
- darknet marketplace links;
- ransomware exposure;
- fraud indicators;
- theft reports;
- scam exposure;
- mixer interaction;
- illicit marketplace activity;
- terrorism financing indicators; and
- other financial crime intelligence.

Wallet risk assessments shall form part of the overall customer risk assessment but shall not be relied upon as the sole basis for regulatory decisions.

12.6 Ongoing Monitoring

The Operator shall monitor cryptocurrency activity throughout the customer relationship.

Monitoring may include:

- transaction frequency;
- cumulative transaction values;
- gaming activity;
- deposit and withdrawal patterns;
- changes in wallet behaviour;
- blockchain intelligence updates;
- unusual transaction timing;
- rapid movement of funds; and
- other relevant behavioural indicators.

Where material changes are identified, the customer's risk profile shall be reviewed.

12.7 Enhanced Due Diligence

Enhanced Due Diligence (EDD) shall be applied where higher cryptocurrency-related risks are identified.

EDD measures may include:

- obtaining additional identity documentation;
- enhanced source of funds verification;
- source of wealth enquiries;
- additional blockchain investigations;
- review of historical transactions;
- management approval prior to continuing the business relationship;
- increased transaction monitoring; and
- temporary suspension of withdrawals where appropriate.

EDD measures shall remain proportionate to the assessed level of risk.

12.8 High-Risk Cryptocurrency Activity

Examples of cryptocurrency activities requiring enhanced review include:

- unusually large transactions;
- rapid deposits followed by immediate withdrawals;
- minimal gaming activity relative to transaction volumes;
- repeated use of newly created wallet addresses;
- transactions linked to high-risk jurisdictions;
- repeated interaction with higher-risk counterparties;
- structuring designed to avoid internal controls;
- unusual transaction velocity;
- attempts to circumvent verification requirements; or
- any activity giving rise to reasonable suspicion of financial crime.

The presence of one or more indicators shall not automatically result in account closure but shall require further assessment.

12.9 Suspicious Activity Reporting

Employees who identify potentially suspicious cryptocurrency activity shall immediately report the matter to the MLRO.

The MLRO shall determine whether:

- additional enquiries are required;
- enhanced due diligence should be performed;
- the business relationship should continue;
- transactions should be delayed where legally permissible; or
- a Suspicious Activity Report (SAR) or equivalent report should be submitted to the competent authority.

Employees shall not disclose to players that a suspicious activity review or regulatory report is being considered or has been submitted.

12.10 Sanctions Compliance

All cryptocurrency activities shall remain subject to the Operator's Sanctions Policy.

Where sanctions concerns arise, the Operator may:

- suspend deposits;
- suspend withdrawals;
- request additional information;
- block transactions where legally required;
- report to competent authorities where applicable; and
- terminate the business relationship where appropriate.

Sanctions compliance shall be monitored on an ongoing basis.

12.11 Record Keeping

The Operator shall maintain appropriate AML/CFT records relating to cryptocurrency activities.

Records may include:

- customer due diligence documentation;
- wallet screening results;
- blockchain analytics reports;
- sanctions screening records;
- source of funds documentation;
- source of wealth documentation;
- enhanced due diligence records;
- internal investigation records;
- suspicious activity reports; and
- management approvals.

Records shall be retained for the period required by applicable law and the Operator's Record Retention Policy.

12.12 Independent Review

The effectiveness of cryptocurrency AML/CFT controls shall be reviewed periodically as part of the Operator's overall AML compliance programme.

The review may consider:

- effectiveness of blockchain analytics;
- quality of customer due diligence;
- effectiveness of transaction monitoring;
- sanctions controls;
- staff awareness;
- emerging financial crime typologies;
- regulatory developments; and
- recommendations arising from internal or external audits.

Appropriate remedial action shall be implemented where deficiencies are identified.

13. INCIDENT RESPONSE & BUSINESS CONTINUITY

13.1 Purpose

The Operator shall maintain procedures to identify, respond to, mitigate, recover from, and document incidents affecting cryptocurrency operations.

Incident management shall minimise disruption to licensed gaming activities while protecting player assets, maintaining regulatory compliance, and preserving business continuity.

13.2 Scope

This Chapter applies to incidents involving:

- cryptocurrency wallets;
- blockchain infrastructure;
- treasury operations;
- payment processing;
- cybersecurity;
- blockchain analytics;
- digital asset custody;
- third-party cryptocurrency service providers; and
- any event affecting the integrity or availability of cryptocurrency services.

13.3 Examples of Incidents

Examples include, but are not limited to:

- suspected wallet compromise;
- private key exposure;
- unauthorised transactions;
- blockchain network outages;
- blockchain forks materially affecting operations;
- ransomware attacks;
- phishing attacks;
- malware infections;
- denial-of-service attacks;
- stablecoin de-pegging events;
- significant failures of third-party service providers;
- erroneous cryptocurrency transfers;
- prolonged withdrawal disruption; and
- cybersecurity incidents affecting cryptocurrency infrastructure.

13.4 Incident Response

Upon identification of a material incident, the Operator shall:

- assess the nature and severity of the incident;
- contain the incident where possible;
- protect player assets;
- preserve relevant evidence;
- notify appropriate internal stakeholders;
- engage relevant technical specialists where necessary;
- restore services safely; and
- document lessons learned.

13.5 Regulatory Notification

Where required by applicable law or licence conditions, the Operator shall notify the Curaçao Gaming Authority and other competent authorities within the required timeframe.

13.6 Business Continuity

Business Continuity procedures shall support continued operation of critical cryptocurrency services.

These procedures may include:

- backup wallet infrastructure;
- redundant systems;
- alternative communication procedures;
- contingency treasury arrangements;
- disaster recovery procedures;
- restoration testing; and
- emergency operational governance.

Business Continuity arrangements shall be tested periodically.

14. CYBERSECURITY CONTROLS

14.1 General Principles

Cryptocurrency infrastructure shall be protected using appropriate administrative, physical, and technical safeguards.

Cybersecurity controls shall follow recognised industry standards and be proportionate to the Operator's risk profile.

14.2 Security Controls

Security measures may include:

- multi-factor authentication;
- endpoint protection;
- encryption;
- privileged access management;
- vulnerability management;
- security patch management;
- network segmentation;
- intrusion detection;
- logging and monitoring; and
- secure configuration management.

14.3 Access Control

Access to cryptocurrency systems shall be restricted to authorised personnel on a need-to-know basis.

Access permissions shall be reviewed periodically and revoked immediately when no longer required.

14.4 Security Testing

The Operator shall periodically conduct:

- vulnerability assessments;
- penetration testing;
- configuration reviews;
- security audits; and
- access control reviews.

Material findings shall be remediated in accordance with the Operator's Information Security Policy.

15. TRAINING & COMPETENCY

15.1 General

Employees involved in cryptocurrency operations shall receive appropriate training before assuming relevant responsibilities.

Training shall be refreshed at least annually or more frequently where significant regulatory or operational changes occur.

15.2 Training Topics

Training may include:

- cryptocurrency fundamentals;
- blockchain technology;
- wallet security;
- treasury procedures;
- AML/CFT obligations;
- sanctions compliance;
- blockchain analytics;
- fraud prevention;
- cybersecurity awareness;
- responsible gaming;
- incident reporting; and
- regulatory developments.

15.3 Training Records

Training attendance, completion, and competency assessments shall be documented and retained in accordance with the Operator's Record Retention Policy.

16. RECORD RETENTION

16.1 General

The Operator shall maintain complete, accurate, and readily retrievable records relating to cryptocurrency operations.

Records shall be protected against unauthorised alteration, destruction, or loss.

16.2 Records

Records may include:

- wallet registers;
- treasury records;
- blockchain transaction records;

- blockchain transaction hashes;
- reconciliation reports;
- customer due diligence documentation;
- blockchain analytics reports;
- sanctions screening results;
- source of funds documentation;
- incident reports;
- internal approvals;
- audit reports;
- policy reviews;
- training records; and
- third-party due diligence documentation.

16.3 Retention Period

Records shall be retained for the minimum period required by applicable laws, regulations, licence conditions, and the Operator's Record Retention Policy.

Where multiple retention requirements apply, the longer period shall prevail.

16.4 Regulatory Access

Records shall be made available to the Curaçao Gaming Authority and other competent authorities upon lawful request.

17. POLICY GOVERNANCE & REVIEW

17.1 Ownership

This Policy is owned by the Compliance Department.

Operational responsibility is shared between Compliance, Finance, Treasury, Information Technology, Security, and Senior Management.

17.2 Review

This Policy shall be reviewed at least annually.

An earlier review shall be conducted whenever there is:

- a significant regulatory development;

- introduction of a new cryptocurrency;
- implementation of new wallet technology;
- material cybersecurity incidents;
- significant AML/CFT developments;
- changes to the Operator's business model; or
- directions issued by the Curaçao Gaming Authority.

17.3 Version Control

All amendments shall be:

- documented;
- version controlled;
- approved by Senior Management or the Board where appropriate; and
- communicated to relevant personnel before implementation.

17.4 Exceptions

Any exception to this Policy shall:

- be documented;
- include an appropriate risk assessment;
- receive documented management approval; and
- be reviewed periodically until closed.

APPENDIX A – DEFINITIONS

For the purposes of this Policy:

Blockchain means a distributed ledger technology recording cryptocurrency transactions.

Cold Wallet means a cryptocurrency wallet maintained offline or otherwise isolated from internet-connected infrastructure.

Hot Wallet means a cryptocurrency wallet connected to operational systems for processing routine transactions.

Private Key means confidential cryptographic credentials used to authorise cryptocurrency transactions.

Treasury Wallet means a wallet used to manage operational cryptocurrency reserves.

Virtual Asset Service Provider (VASP) has the meaning assigned under applicable legislation.