

TC ENTERTAINMENT N.V.

CRYPTO POLICY

Version 1.0

Document control item	Details
Licensee	TC Entertainment N.V. (the "Company")
Brand / domain	Hititbet / www.hititbet.com
Policy owner	Compliance Officer / MLRO
Approved by	<i>Board of Directors</i>
Effective date	01.07.2026
Next scheduled review	01.07.2027
CGA portal upload date	01.07.2026
Classification	Confidential - internal compliance policy

Contents

1. 1. Purpose, scope and regulatory basis
 2. 2. Key definitions
 3. 3. Governance, accountability and sign-off
 4. 4. Prohibition on acting as a financial institution, exchange or VASP
 5. 5. Crypto AML/KYC framework
 6. 6. Blockchain analytics and transaction monitoring capability
 7. 7. Digital assets and transaction sources
 8. 8. FATF Travel Rule compliance
 9. 9. Third-party VASPs, exchanges, custodians and payment providers
 10. 10. Unhosted wallets and DeFi exposure
 11. 11. Transaction management, deposits and withdrawals
 12. 12. Operator wallets, segregation and reconciliation
 13. 13. Hot, warm and cold wallet controls
 14. 14. Incident reporting and escalation
 15. 15. Records, audit trail and data retention
 16. 16. Staff training
 17. 17. Compliance implementation timeline
 18. 18. Review and change management
- Annexes

1. Purpose, Scope and Regulatory Basis

1.1 Purpose

This Crypto Policy (the "Policy") sets out the controls adopted by TC Entertainment N.V. (the "Company") for accepting, screening, holding, reconciling and paying out crypto-assets in connection with its remote gambling operations under its Curaçao Gaming Authority ("CGA") B2C licence.

The purpose of this Policy is to ensure that crypto-related workflows are transparent, traceable, risk-assessed, auditable and consistent with the Company's AML/CFT, KYC, sanctions, responsible gaming, player protection, operational resilience and incident reporting obligations.

1.2 Scope

This Policy applies to all crypto-asset workflows connected to the licensed operation, including deposits, wagering, withdrawals, player refunds, treasury transfers, wallet management, third-party VASP arrangements, blockchain analytics, transaction monitoring, incident reporting and record-keeping.

This Policy applies to TC Entertainment N.V., its directors, officers, employees, contractors, outsourced service providers, payment partners, group entities supporting the licensed operation, and any approved third party involved in crypto processing for the Company.

1.3 Regulatory basis

This Policy has been prepared with reference to the CGA Crypto Policy Guideline for Online Gaming Operators, June 2026. It does not replace the Company's obligations under Curaçao law, the National Ordinance on Games of Chance, the Company's licence conditions, AML/CFT regulations, sanctions obligations, responsible gaming rules, data protection obligations, VASP-related laws, or any other applicable legal or regulatory requirement.

The Company shall independently assess whether any crypto-related activity triggers registration, licensing, reporting or other obligations under Curaçao VASP laws or any other applicable framework.

1.4 Core principles

- Crypto payments are accepted only as a payment method for gambling services and not as a financial service.
- The Company does not act as an exchange, payment services provider, custodian, wallet provider, broker, dealer, remittance service or VASP for players.
- All accepted crypto-assets must be subject to documented asset-specific risk assessment.
- All crypto deposits and withdrawals must be screened and monitored using blockchain analytics capability.
- Prohibited assets and prohibited transaction sources must be rejected, frozen or returned in accordance with this Policy and applicable law.
- Player funds and Company funds must be segregated and reconciled.
- Outsourcing may support the control framework, but accountability remains with the Company.

2. Key Definitions

Term	Definition
Virtual Asset Service Provider (VASP)	A legal or natural person that conducts exchange between virtual assets and fiat currencies, exchange between virtual assets, transfer of virtual assets, safekeeping or administration of virtual assets, or instruments enabling control over virtual assets on behalf of another person.
Unhosted wallet	A self-hosted or non-custodial wallet that is not managed by a VASP and is controlled directly by a user through private keys.
Wallet ownership verification	The process of confirming that a player controls a specific wallet address, using methods such as test transactions, signed messages, whitelisting, or equivalent controls.
Blockchain analytics tool	A system or service capable of tracing, analysing, risk-scoring and evidencing virtual asset transactions, including exposure to high-risk or prohibited sources.

FATF Travel Rule	The requirement that originator and beneficiary information accompanies applicable virtual asset transfers between regulated entities and is made available to competent authorities upon request.
Compliant VASP	A VASP that demonstrates appropriate AML/CFT controls, Travel Rule capability, sanctions screening, transaction monitoring, operational resilience and transparency, assessed on a risk-based basis.
Prohibited source	A wallet, transaction, service, asset, chain, protocol or counterparty that is sanctioned, linked to criminal activity, linked to mixers or tumblers, privacy-enhanced in a way that prevents adequate monitoring, or otherwise unacceptable under this Policy.
Player-flow wallet	A wallet used for player deposits, player withdrawals or player refunds.
Operational wallet	A wallet used for liquidity management or operational transfers connected to the licensed operation.
Treasury wallet	A wallet used for reserves, long-term safeguarding or non-day-to-day custody of Company or segregated player funds.

3. Governance, Accountability and Sign-Off

3.1 Ownership and approval

This Policy is owned by the Compliance Officer / MLRO and must be approved by the Board of Directors before implementation. The effective date, approval date and next scheduled review date must be recorded in the Document Control Table.

3.2 Responsibility matrix

Role	Responsibilities
Board of Directors	Approves this Policy, receives material risk updates, approves material changes and ensures adequate resources.
Compliance Officer / MLRO	Owns the Policy, oversees AML/CFT controls, sanctions controls, blockchain analytics, escalations, suspicious activity reporting and CGA reporting.
Finance / Treasury	Maintains wallet inventory, reconciliations, liquidity controls, payment records, VASP records and segregation of funds.
Crypto Operations / Payments Team	Processes deposits and withdrawals, applies wallet whitelisting, performs operational checks and escalates exceptions.
Risk / Fraud Team	Monitors high-risk patterns, fraud indicators, collusion, chip dumping, chargeback abuse and suspicious transaction patterns.
IT / Security	Implements access controls, MFA, key management, wallet security, incident containment and system logs.
Customer Support	Collects player information, communicates document requests and escalates KYC, withdrawal and complaint issues.
Outsourced providers	Perform contracted services only, subject to due diligence, oversight, confidentiality and audit rights.

3.3 Change management

Any addition or removal of an accepted crypto asset, token, blockchain network, wallet, VASP, exchange, custodian, payment provider, risk threshold, withdrawal rule or blockchain analytics provider requires a documented risk assessment and appropriate sign-off before implementation.

The Compliance Officer / MLRO must record the reason for the change, risk impact, effective date, approval, affected systems, player-facing impact and whether any CGA notification or portal update is required.

3.4 Unscheduled review triggers

- Material change to CGA guidance, Curaçao law, AML/CFT rules, sanctions requirements or VASP regulation.
- Addition or removal of accepted crypto assets, networks, wallets, VASPs or payment providers.

- Material crypto incident, security breach, wallet compromise or exposure to prohibited sources.
- Material increase in crypto transaction volumes, high-risk jurisdictions or higher-risk player profiles.
- Blockchain fork, chain disruption, stablecoin depeg, delisting event or material volatility event.
- Internal audit, external audit, regulator request or identified control weakness.

4. Prohibition on Acting as a Financial Institution, Exchange or VASP

4.1 No financial services

The Company accepts crypto-assets only as a payment method for participation in gambling services. The Company must not function as a financial institution, exchange, broker, dealer, payment services provider, remittance service, custodian, wallet provider or VASP for players.

4.2 Prohibited activities

- The Company must not convert crypto to crypto or crypto to fiat for players as a standalone service.
- The Company must not offer trading, swapping, exchange, investment, lending, staking, yield or brokerage services.
- The Company must not offer custody, transfer or wallet services outside gambling-related transactions.
- The Company must not hold player crypto balances for a purpose unrelated to gambling services.
- The Company must not enable player-to-player transfers on the platform.

4.3 Player disclosure

The Company shall make clear in its player-facing Terms and Conditions and payment pages that it is not responsible for exchange, brokerage, wallet, custody, token purchase, token sale, fiat conversion or other services provided by third-party exchanges, wallets, payment providers or VASPs used by a player.

5. Crypto AML/KYC Framework

5.1 No crypto carve-out

The use of crypto-assets does not reduce or replace the Company's AML/CFT, KYC, sanctions, fraud prevention, responsible gaming, player protection or reporting obligations. Crypto transactions are treated as high risk unless the Company's documented risk assessment supports a lower risk rating for a specific player, asset, VASP and transaction flow.

5.2 KYC requirements

The Company shall apply customer due diligence to players who use crypto deposits or withdrawals. KYC may include identity verification, age verification, address verification, payment method verification, wallet ownership verification, source of funds, source of wealth, sanctions screening, PEP screening, adverse media screening and ongoing monitoring.

5.3 Crypto-specific triggers for enhanced due diligence

- Use of unhosted wallets or DeFi protocols where elevated risk is identified.
- Exposure to high-risk wallet clusters, darknet markets, scams, fraud, ransomware, stolen funds, mixers, tumblers or sanctioned entities.
- Large, unusual, complex, rapid, circular, structured or economically irrational crypto transactions.
- Use of a VASP that does not demonstrate adequate AML/CFT, sanctions screening, Travel Rule capability or transparency.
- Attempted withdrawal to a new wallet that has not been whitelisted or verified.
- Deposit and withdrawal patterns suggesting money laundering, chip dumping, collusion, bonus abuse or player-to-player value transfer.

- Use of assets with material volatility, low liquidity, anonymity features, bridged provenance uncertainty or manipulation indicators.
- Transaction activity inconsistent with the player's profile, declared source of funds or expected play behaviour.

5.4 Source of funds and source of wealth

Where required by risk, threshold, regulation or internal policy, the Company shall request evidence to establish the source of funds and, where appropriate, source of wealth connected to crypto activity. Evidence may include exchange statements, wallet history, transaction hashes, bank statements, salary evidence, business income evidence, sale-of-asset evidence, inheritance evidence, tax documentation, proof of mining income, investment records or other reliable documents.

5.5 Suspicious activity

The Company shall investigate unusual or suspicious crypto activity and, where required, file reports with the relevant competent authority. The Company may freeze, reject, return, delay or block funds where required by law, sanctions, AML/CFT obligations, fraud prevention, CGA requirements or this Policy.

6. Blockchain Analytics and Transaction Monitoring Capability

6.1 Minimum functionality

The Company shall maintain blockchain analytics capability through an internal system, an external provider or a combination of systems. The Company may use providers such as Chainalysis, Elliptic, TRM Labs or an equivalent solution, provided that the required functionality is achieved.

Functionality	Control requirement
Fund tracing	Trace the origin and destination of funds, including prior hops and onward exposure where appropriate.
Risk scoring	Assess and risk-score wallets, transactions, clusters, VASPs, protocols and sources.
Deposit screening	Screen sending wallets and transaction sources at the point of deposit.
Withdrawal screening	Screen destination wallets before outbound transfers.
Ongoing monitoring	Detect new risk exposure, linked wallets and suspicious patterns over time.
Source of funds support	Trace fund origins and retain evidence for KYC, EDD, reporting and audit purposes.
Suspicious activity investigation	Evidence suspicious activity, exposure to prohibited sources and decisions taken.
Sanctions and prohibited source detection	Identify exposure to sanctioned wallets, mixers, tumblers, darknet markets, scams, fraud-linked wallets and other prohibited sources.

6.2 Risk-rating framework

Risk level	Indicators	Required action
Low	Transparent source, approved asset, verified player, compliant VASP, no adverse exposure.	Process subject to normal monitoring.
Medium	Limited exposure to elevated-risk indicators or incomplete contextual information.	Request additional information, monitor and escalate if unresolved.
High	Material risk indicators, unhosted wallet complexity, high-risk VASP, unusual pattern or source of funds concern.	Escalate to Compliance Officer / MLRO; apply EDD; delay transaction pending review.
Prohibited	Sanctions exposure, mixer/tumbler exposure, darknet, fraud-linked wallet, ransomware, stolen funds, prohibited asset or blocked jurisdiction.	Reject, freeze, return or block as legally appropriate; consider suspicious activity and incident reporting.

6.3 Evidence standard

The Company must retain an audit trail showing the transaction hash, wallet addresses, screening result, risk score, reason for decision, evidence reviewed, staff member handling the review, approval obtained, final action and any report submitted.

7. Digital Assets and Transaction Sources

7.1 Asset-specific approval

The Company shall not accept any crypto asset unless the asset has been approved through the asset risk assessment process. Preference shall be given to fiat-backed regulated stablecoins and other transparent, liquid, auditable assets where the Company can meet its AML/CFT, monitoring, record-keeping and player protection obligations.

7.2 Asset risk criteria

- Transparency and traceability of the blockchain or token network.
- Liquidity, market depth, volatility profile and risk of manipulation.
- Availability of reliable blockchain analytics coverage.
- Sanctions, fraud, darknet, scam and illicit finance exposure.
- Governance, issuer credibility, reserves and redemption profile for stablecoins.
- Technical risks, smart contract risks, chain stability and operational resilience.
- Whether the asset is privacy-enhancing, wrapped, bridged, pooled or otherwise difficult to attribute.

7.3 Privacy-enhancing cryptocurrencies

The Company shall not accept assets or transaction types that prevent effective monitoring, blockchain analysis or source-of-funds verification. This includes Monero, Zcash shielded transactions, Dash where privacy features are used, Litecoin MWEB where privacy functionality is used, and any other asset or feature that materially obscures transaction data.

7.4 Pooled or omnibus wallets

Pooled or omnibus wallet structures operated by VASPs may be accepted only where the Company can obtain sufficient data to attribute transactions to the relevant player, assess source of funds, monitor transactions and meet reporting obligations. Structures that prevent effective attribution, monitoring or auditability are not permitted.

7.5 Meme or highly speculative tokens

The Company shall apply enhanced asset review before accepting meme coins or highly speculative tokens. Such tokens may be accepted only where objective and observable criteria demonstrate sufficient liquidity, transparent transaction history, acceptable volatility profile, sufficient blockchain analytics coverage, no anonymity-enhancing design, no material manipulation concern and no unacceptable financial-crime exposure.

7.6 Wrapped tokens and bridged assets

The Company shall not accept wrapped tokens or bridged assets where the provenance, custody, backing or transaction history of the underlying asset cannot be independently verified. Wrapped or bridged assets must be assessed for counterparty risk, bridge risk, smart contract risk, provenance opacity, backing risk and potential disconnection from the underlying asset's transaction history.

7.7 Expressly prohibited sources and assets

- Sanctioned wallets, sanctioned entities, sanctioned jurisdictions or blocked addresses.
- Sanctioned cryptocurrency mixers, tumblers or anonymity services.

- Wallets flagged by recognised blockchain analytics providers as linked to darknet markets, ransomware, scams, fraud, terrorist financing, child exploitation material, stolen funds or other serious crime.
- Privacy-enhancing assets or features that prevent adequate traceability.
- Assets, token types, chains or mechanisms designated as prohibited by the CGA or by the Company's Compliance Officer / MLRO.

8. FATF Travel Rule Compliance

8.1 General obligation

Where the FATF Travel Rule applies to a transfer between regulated entities, including exchanges, custodial wallet providers and VASPs, required originator and beneficiary information must accompany the transfer and must be made available to competent authorities upon request.

8.2 Company control requirements

- The Company shall assess whether a VASP used for player deposit or withdrawal flows has Travel Rule capability appropriate to the risk of the relationship.
- The Company shall collect, retain and make available originator and beneficiary information where required by law, VASP arrangements or internal controls.
- The Company shall not knowingly process a transaction where required Travel Rule information is missing and the risk cannot be remediated.
- The Company shall document Travel Rule exceptions, rejected transfers and related compliance decisions.

9. Third-Party VASPs, Exchanges, Custodians and Payment Providers

9.1 Outsourcing and accountability

The Company may use third-party VASPs, exchanges, custodians, payment providers, wallet infrastructure providers or blockchain analytics providers. However, the use of third parties does not transfer, reduce or dilute the Company's AML/CFT, KYC, sanctions, transaction monitoring, player protection, incident reporting or CGA obligations.

9.2 Due diligence standards

- Regulatory status, registration, licensing or reputable oversight in the provider's home jurisdiction.
- AML/CFT policy, sanctions screening, PEP screening and transaction monitoring controls.
- Travel Rule capability, wallet screening and suspicious activity escalation procedures.
- Operational resilience, cyber security, key management, business continuity and disaster recovery.
- Transparency, auditability, reporting capability and availability of transaction data.
- Data protection, confidentiality, access rights, service levels, audit rights and termination rights.
- Financial stability, reputation, adverse media and litigation/regulatory history.

9.3 Ongoing monitoring

Third-party providers must be reviewed at onboarding and periodically thereafter. Material incidents, regulatory actions, adverse media, control failures, service outages, sanctions exposure or change of ownership must trigger an out-of-cycle review.

10. Unhosted Wallets and DeFi Exposure

10.1 Acceptance subject to controls

The Company may accept crypto-assets from unhosted wallets or DeFi protocols only where risk-based controls allow the Company to meet its AML/CFT, sanctions, transaction monitoring, KYC and reporting obligations.

10.2 Minimum controls

- Verify wallet ownership or control using test transactions, signed messages, whitelisting, cryptographic proof or equivalent mechanisms.
- Apply blockchain analytics to assess the wallet and transaction history before accepting deposits or processing withdrawals.
- Require enhanced due diligence where elevated risk indicators are identified.
- Reject, freeze, return or block transactions where monitoring, attribution or reporting obligations cannot be met.
- Screen DeFi protocols, smart contracts, liquidity pools, bridges and counterparties where relevant.

10.3 Wallet whitelisting

Before processing withdrawals to an unhosted wallet, the Company must verify that the wallet belongs to or is controlled by the same player, screen the wallet, record the screening result and whitelist the address where appropriate. Whitelisting must be reviewed periodically and after any risk trigger.

11. Transaction Management, Deposits and Withdrawals

11.1 Deposits

Crypto deposits shall be accepted only in approved assets, on approved networks and through approved wallets or payment providers. The Company shall screen deposit wallets and transaction sources using blockchain analytics before crediting or making funds available for play, subject to operational thresholds and risk-based controls.

11.2 Withdrawals

The default expectation is that withdrawals are processed to the same wallet and in the same crypto asset as the original deposit. Where this is not possible, the Company may use a permitted alternative approach only where equivalent controls can be demonstrated and documented.

11.3 Alternative withdrawal approaches

- Withdrawal to a different wallet is permitted only where the wallet is whitelisted, pre-screened, verified as belonging to the same player and has passed KYC/AML checks.
- Withdrawal in a different crypto asset or stablecoin is permitted only where the full transaction flow remains transparent and auditable, conversion is conducted by a regulated or compliant VASP, and records are retained.
- Withdrawal to a third-party wallet is prohibited unless required by law, court order or regulatory instruction and approved by the Compliance Officer / MLRO.
- Player-to-player transfers on the platform are prohibited.

11.4 Transaction exception handling

Scenario	Required handling
High-risk deposit	Hold or delay crediting; escalate to Compliance Officer / MLRO; request KYC/EDD; reject, freeze or return if required.
Prohibited source detected	Block, freeze, reject or return as legally appropriate; assess suspicious activity and incident reporting.
Wallet mismatch	Do not process withdrawal until wallet ownership is verified and whitelisting is completed.
Unsupported asset/network	Do not credit automatically; assess recoverability; communicate to player; record decision.
Blockchain congestion/outage	Delay processing; communicate where appropriate; monitor chain status; record incident if material.
Fork, bridge failure or smart contract incident	Suspend affected asset/network; assess exposure; escalate and report if required.

12. Operator Wallets, Segregation and Reconciliation

12.1 Wallet ownership and control

All wallets used in connection with the licensed operation must be owned or controlled by TC Entertainment N.V. or an approved group/payment entity documented in the wallet register. Personal wallets, UBO-linked wallets, employee wallets and informal wallet arrangements are prohibited.

12.2 Wallet segregation

The Company shall segregate wallet functions to distinguish player-flow wallets, operational wallets and treasury wallets. Player funds shall be held in segregated wallets to support accountability and prevent commingling of player funds and Company funds.

12.3 Wallet register

The Company shall maintain an up-to-date wallet register recording the wallet address, blockchain network, wallet type, purpose, owner/controller, access rights, authorised signers, linked VASP/provider, approval date, status, risk rating and reconciliation frequency.

12.4 Reconciliation

- Player-flow wallets must be reconciled at least daily or at a frequency proportionate to transaction volume and risk.
- Operational and treasury wallets must be reconciled at least monthly and after any material transfer.
- Material discrepancies must be escalated immediately to Finance, the Compliance Officer / MLRO and IT/Security.
- Reconciliation records must be retained and made available for audit and regulatory review.

13. Hot, Warm and Cold Wallet Controls

Wallet type	Control standard
Hot wallets	Used for day-to-day player deposits and withdrawals. Balances must be limited to operationally necessary amounts. Access must be tightly controlled and monitored.
Warm wallets	Used for liquidity management. Subject to enhanced access controls, approval procedures, whitelisting and reconciliation.
Cold wallets	Used for treasury, reserves or longer-term safeguarding. Access, key management, approvals, reconciliation and auditability must be maintained.

13.1 Security controls

- Multi-signature controls must be used where proportionate to value and risk.
- MFA, hardware security modules, secure key custody or equivalent controls must be applied where appropriate.
- Withdrawal whitelisting must be used for operational and treasury transfers where feasible.
- Access rights must be role-based, documented, approved and reviewed periodically.
- Private keys, seed phrases and recovery information must not be stored in plain text, email, shared drives or personal devices.
- Emergency access procedures must be documented, dual-controlled and auditable.
- Movement between wallets must be approved, recorded, reconciled and supported by transaction hashes.

14. Incident Reporting and Escalation

14.1 Incident identification

Crypto-related incidents must be identified, assessed, escalated and reported in accordance with the Company's Incident Reporting Policy, the National Ordinance on Games of Chance and applicable CGA requirements, including Article 5.10 Incident Reporting where applicable.

14.2 Reportable incidents

- Compromised private keys, wallet access or unauthorised transactions.
- Security breaches affecting wallets, VASPs, payment providers, exchanges, blockchain analytics tools or internal systems.
- System failures affecting crypto processing, including exchange outages, blockchain congestion or failed transactions.
- Fraud schemes involving crypto, including coordinated deposit/withdrawal patterns, chip dumping, collusion or suspicious circular flows.
- Material discrepancies in wallet balances, transaction records or reconciliations.
- Exposure to sanctioned wallets, mixers, tumblers, prohibited sources or prohibited assets.
- Smart contract failures, blockchain forks, bridge failures or chain-level disruptions.
- Any event that may affect the integrity, security, transparency or traceability of crypto transactions.

14.3 Escalation timeline

Step	Action	Owner
1	Identify and contain the incident; preserve logs and evidence.	First responder / IT / Payments
2	Notify Compliance Officer / MLRO, IT/Security and senior management.	Incident owner
3	Assess player impact, financial impact, AML/CFT impact and CGA reporting requirement.	Compliance Officer / MLRO
4	Freeze, block, suspend or isolate affected wallets, assets or providers where required.	IT / Finance / Compliance
5	Submit regulatory, suspicious activity or law enforcement reports where required.	Compliance Officer / MLRO
6	Complete root cause analysis and remediation plan.	Management / Policy owner

15. Records, Audit Trail and Data Retention

15.1 Record-keeping requirement

The Company shall maintain records sufficient to evidence ownership/control, transaction history, screening results, risk ratings, KYC/EDD actions, source of funds reviews, approvals, reconciliations, wallet movements, incidents, reports, VASP due diligence, asset approvals, player communications and policy changes.

15.2 Minimum records

- Player KYC, wallet ownership verification and EDD records.
- Deposit and withdrawal transaction hashes, wallet addresses, assets, networks, timestamps and amounts.
- Blockchain analytics screening reports, risk scores and decision logs.
- VASP, exchange, custodian, payment provider and analytics provider due diligence records.
- Approved asset risk assessments and changes to accepted assets or networks.
- Wallet register, access rights, approval logs and reconciliation records.
- Incident records, suspicious activity reports, CGA reports and remediation evidence.
- Staff training records and competence assessments.

15.3 Retention period

Crypto-related records shall be retained for at least the period required by applicable law, licence conditions, AML/CFT requirements, tax requirements and regulatory obligations. Unless a longer period is required, the Company shall retain crypto compliance records for at least [insert retention period, e.g. five years after account closure or transaction completion].

16. Staff Training

16.1 Training requirement

Relevant personnel must be trained in digital asset risk identification and assessment, including crypto AML/CFT risks, blockchain analytics outputs, sanctions exposure, wallet ownership verification, Travel Rule considerations, prohibited assets, prohibited sources, incident escalation and record-keeping.

16.2 Training frequency

Crypto training shall be provided at onboarding and at least annually thereafter. Additional training shall be provided when this Policy is materially updated, when new assets or providers are approved, after a material incident, or when regulatory changes require additional controls.

17. Compliance Implementation Timeline

The Company shall implement this Policy according to the phased timeline below, unless the CGA requires earlier implementation or the Company identifies material risk requiring accelerated implementation.

Phase	Requirement
Immediate effect	Prohibitions on sanctioned wallets, mixers, prohibited crypto assets, personal wallets, UBO-linked wallets and acting as an exchange, payment provider or VASP.
By September 2026	Upload this Crypto Policy to the CGA portal and maintain a clear timeline for adoption and compliance with the CGA Crypto Policy Guideline.
By December 2026	Complete documented crypto risk assessments, VASP due diligence, wallet ownership controls, transaction monitoring procedures and staff training.
By June 2027	Fully implement wallet segregation, blockchain analytics capability, reconciliation processes, withdrawal whitelisting or equivalent controls and audit-ready record-keeping.

18. Review and Change Management

18.1 Scheduled review

This Policy shall be reviewed at least annually by the Compliance Officer / MLRO and approved by the Board where material changes are required.

18.2 Version control

The Company shall maintain a version history recording all material changes, effective dates, approvers and reasons for change.

Version	Date	Description of change	Approved by
1.0	01.07.2026	Initial Crypto Policy prepared in accordance with the CGA Crypto Policy Guideline for Online Gaming Operators, June 2026.	Board of Directors

Annex 1 -

Asset risk assessment checklist:

- Is the asset transparent and traceable using the Company's blockchain analytics capability?
- Is the asset liquid and sufficiently stable for player fund purposes?
- Does the asset include privacy-enhancing, anonymity or obfuscation features?
- Is the asset wrapped, bridged, synthetic, algorithmic or dependent on external custody/backing?
- Is the asset exposed to sanctions, mixers, scams, fraud, darknet markets or other prohibited sources?
- Is the asset supported by approved wallets, VASPs, payment providers and reconciliation systems?

Annex 2 - Prohibited Assets and Sources

Category	Policy position
Sanctioned wallets / entities	Prohibited. Reject, freeze, return or block as legally appropriate; escalate to Compliance Officer / MLRO.
Mixers / tumblers	Prohibited, including sanctioned mixers and anonymity services.
Privacy coins / shielded transactions	Prohibited where effective transaction monitoring or source-of-funds verification is impaired.
Darknet / fraud / ransomware / stolen funds exposure	Prohibited or high risk requiring escalation and likely rejection/freezing.
Unverified wrapped or bridged assets	Prohibited where provenance, custody, backing or history cannot be verified.
Personal / UBO / employee wallets for operator funds	Prohibited.

Annex 3 - Wallet Register Template

Wallet address	Network	Wallet type	Purpose	Owner/controller	Risk rating
[insert]	[insert]	[Hot / warm / cold]	[Player-flow / operational / treasury]	[insert]	[insert]
[insert]	[insert]	[Hot / warm / cold]	[Player-flow / operational / treasury]	[insert]	[insert]

Annex 5 - Crypto Incident Report Template

Field	Details
Incident reference	[insert]
Date/time identified	[insert]
Detected by	[insert]
Incident type	[Security / prohibited source / outage / fraud / reconciliation discrepancy / other]
Assets, wallets and providers affected	[insert]
Player impact	[insert]
Financial impact	[insert]
Immediate containment action	[insert]
Compliance assessment	[insert]
Reports submitted	[CGA / FIU / law enforcement / VASP / other / not required]
Root cause and remediation	[insert]
Closure approval	[insert]

Annex 6 - Training Register Template

Staff member	Role	Training topic	Date completed	Assessment / notes
<i>[insert]</i>	<i>[insert]</i>	<i>[insert]</i>	<i>[insert]</i>	<i>[insert]</i>
<i>[insert]</i>	<i>[insert]</i>	<i>[insert]</i>	<i>[insert]</i>	<i>[insert]</i>