



CRYPTO RISK MANAGEMENT POLICY

Enterprise-grade policy framework for cryptocurrency acceptance, transaction monitoring, custody, treasury exposure, third-party risk, sanctions, Travel Rule, incident response and governance.

Version 2.0 Draft for Approval | Confidential - Internal Use Only

This policy is written for enterprise implementation. It defines mandatory control outcomes, accountabilities and escalation requirements. Procedures, system configurations and operating checklists must be maintained separately and evidence compliance with this policy.

Document Control

Field	Details
Document Title	Crypto Risk Management Policy
Company	Geeker Technology N.V.
Document Owner	Risk & Compliance Department
Executive Sponsor	CFO / COO
Control Functions	Chief Risk Officer, Chief Compliance Officer, MLRO, Chief Information Security Officer
Version	2.0 - Enterprise Revision Draft
Effective Date	29/06/2025; to be re-confirmed on approval of Version 2.0
Prepared / Revised Date	16/06/2026
Last Review Date	16/06/2026
Next Review Date	16/06/2027, or sooner upon a triggering event
Review Frequency	Annually, and upon regulatory change, material incident or business change
Classification	Confidential - Internal Use Only
Approval Authority / Requirement	Board of Directors or delegated Risk Committee approval, with CFO/COO sign-off

Version History

Version	Date	Author / Owner	Summary of Change	Approval Status
1.0	29/06/2025	Risk & Compliance Department	Initial policy baseline covering scope, governance, broad risk categories, wallet risk, customer risk, reporting and review.	Previously approved in the baseline draft.
2.0	16/06/2026	Risk & Compliance Department	Enterprise-grade rewrite: expanded governance, risk appetite, risk assessment methodology, regulatory perimeter, Travel Rule, sanctions, customer and wallet controls, custody, treasury, vendor risk, cyber controls, incident response, reporting, testing and assurance.	Draft for management/legal/regulatory review and formal approval.

Approval note: Version 2.0 is drafted as a controlled policy document. It should be reviewed by Legal, Compliance, Finance/Treasury, Information Security and Operations before formal adoption. Nothing in this policy should be treated as legal advice, and local regulatory obligations must prevail where stricter than this policy.

Contents

1	Purpose, Scope and Policy Position
2	Regulatory and Standards Basis
3	Governance, Accountability and Three Lines of Defence
4	Risk Appetite and Tolerance Limits
5	Crypto Risk Management Framework
6	Regulatory Perimeter and Permitted Crypto Activities
7	Digital Asset Approval and Product Risk Controls
8	Customer, Wallet and Transaction Risk Management
9	AML/CFT/CPF, Sanctions and Travel Rule Controls
10	Wallet, Custody and Private Key Risk Management
11	Treasury, Market, Liquidity and Stablecoin Risk Management
12	Cybersecurity, Technology and Operational Resilience
13	Third-Party, Custodian and Crypto Payment Provider Risk
14	Accounting, Recordkeeping, Data Protection and Evidence
15	Incident Management, Escalation and Crisis Response
16	Monitoring, Reporting, KRIs and Management Information
17	Training, Awareness, Exceptions and Policy Breaches
18	Assurance, Testing, Review and Approval
App.	Appendices A-H: Definitions, Matrices, Checklists, KRIs, Incident Severity, RACI and Reference Sources

1. Purpose, Scope and Policy Position

Geeker Technology N.V. (the "Company") accepts and processes cryptocurrency and digital asset transactions only where doing so is consistent with applicable law, the Company's gaming licence conditions, its anti-money laundering and counter-terrorist financing obligations, and its approved risk appetite. This Crypto Risk Management Policy establishes the governance, controls and monitoring standards required to identify, assess, mitigate, report and continuously improve the management of crypto-related risks across the Company.

The policy is intended to be read alongside the Company's AML/CFT/CPF Policy, Sanctions Policy, Customer Due Diligence Policy, Responsible Gaming Policy, Information Security Policy, Incident Response Plan, Vendor Risk Management Policy, Treasury Policy, Business Continuity Plan and Data Protection Policy. Where a local law, licence condition, regulator instruction or contractual commitment is stricter than this policy, the stricter requirement applies.

1.1 Objectives

The objectives of this policy are to protect customers, the Company, regulators and the financial system by ensuring that digital asset activity is governed through clear accountability, measurable risk appetite, strong customer and wallet controls, secure custody and transaction processes, timely escalation, effective recordkeeping and independent assurance. The policy also establishes a documented basis for management decisions on crypto asset acceptance, payment providers, wallet infrastructure and treasury exposure.

1.2 Scope

This policy applies to all business units, directors, officers, employees, contractors, consultants and third parties involved in the design, approval, operation, monitoring or oversight of crypto-related activity. It applies regardless of whether activity is performed directly by the Company or through a crypto payment service provider, exchange, custodian, wallet infrastructure provider, blockchain analytics provider or Travel Rule solution provider.

Area	Policy scope
In scope	Customer deposits and withdrawals using digital assets; crypto payment processing; treasury crypto holdings; hot, warm and cold wallets; payment provider and custodian arrangements; blockchain transaction monitoring; Travel Rule and sanctions controls; fraud and AML/CFT/CPF investigations; incident handling; reconciliation; reporting; data retention and independent assurance.
Out of scope unless separately approved	Proprietary speculative trading; market making; customer crypto lending; staking/yield products; crypto derivatives; margin or leveraged crypto activity; DeFi protocol participation; token issuance; initial coin offerings; NFT marketplaces; smart contract deployment; custody services offered to third parties.
Geographic scope	All jurisdictions in which the Company operates, offers services, targets customers, accepts customers or holds licences, including Curaçao and any jurisdiction that applies to customers, payment counterparties, banking partners, CASPs/VASPs, PSPs or custodians used by the Company.

1.3 Core policy position

The Company does not use digital assets as a means to avoid regulation, evade sanctions, obscure customer identity, bypass responsible gaming controls or speculate with corporate funds. Crypto acceptance is permitted only as a controlled payment channel supporting lawful gaming activity. The Company must know its customers, understand the source and destination of funds to a risk-appropriate standard, screen customers and wallets, monitor transactions before and after settlement, maintain secure wallet and custody arrangements, and convert or manage exposures within approved limits.

No new digital asset, wallet infrastructure, custodian, exchange, PSP, blockchain analytics provider, Travel Rule solution, settlement model or crypto-related product feature may be introduced without prior documented risk assessment, Legal and Compliance review, Information Security assessment, Finance/Treasury sign-off and approval under the governance framework set out in this policy.

2. Regulatory and Standards Basis

The digital asset risk environment is fast-moving. The Company therefore adopts a principles-based control framework aligned to internationally recognised AML/CFT, sanctions, cyber, governance and gaming expectations, while reserving the right to implement stricter controls where required by law, regulator expectation, banking partner requirement or Company risk appetite.

The policy has been drafted with regard to FATF standards for virtual assets and VASPs, the FATF Travel Rule, Curaçao Gaming Authority requirements for online gaming and AML/CFT supervision, EU MiCA and Transfer of Funds/Travel Rule standards where applicable, and NIST Cybersecurity Framework principles for cyber risk governance and resilience. These sources are reference points for control design and are not a substitute for jurisdiction-specific legal advice.

Reference area	Policy implication
Curaçao gaming and AML/CFT/CPF framework	The Company must maintain policies and procedures appropriate to its licensing status and must reflect Curaçao Gaming Authority expectations for gaming integrity, AML/CFT supervision, periodic reporting, incident reporting and change reporting where applicable.
FATF virtual asset standards	The Company shall operate a documented risk-based approach for virtual assets, including customer due diligence, transaction monitoring, counterparty due diligence, suspicious transaction reporting, sanctions controls and Travel Rule-related controls where relevant.
EU MiCA and Transfer of Funds / Travel Rule	Where the Company, its PSPs, CASPs, VASPs, customers or services fall within EU scope, applicable MiCA authorisation, conduct, governance, safeguarding, disclosure and Travel Rule information requirements must be assessed and implemented.
Sanctions and targeted financial sanctions	The Company shall screen customers, beneficial owners, wallets, counterparties, geographies, transactions and blockchain exposure against applicable UN, Curaçao, EU, OFAC, UK and other relevant sanctions lists and regulator notifications.
NIST CSF 2.0 / cyber resilience	Wallet infrastructure, private key controls, API connectivity, provider access, security monitoring, incident response and recovery must be governed, identified, protected, detected, responded to and recovered in a manner aligned to enterprise cyber risk management.
Data protection and confidentiality	Customer, blockchain analytics, Travel Rule and investigation data must be handled under appropriate privacy, confidentiality, retention, access control and cross-border transfer safeguards.

Regulatory perimeter principle: The Company must not assume that outsourcing crypto activity to a payment provider eliminates its own AML, sanctions, responsible gaming, customer protection, incident reporting, licence or reputational obligations. Outsourcing transfers performance, not accountability.

3. Governance, Accountability and Three Lines of Defence

Crypto risk management must be embedded in the Company's enterprise risk management framework. Accountability must be clear, documented and evidenced. The Board retains ultimate oversight of the Company's risk appetite and control environment. Management owns implementation. Control functions set standards, monitor adherence and escalate issues. Internal Audit or equivalent independent assurance tests effectiveness.

3.1 Governance bodies and accountable owners

Role / function	Accountability
Board of Directors	Approves the crypto risk appetite, this policy, material changes to crypto strategy, and acceptance of any high or critical residual crypto risk. Receives quarterly and ad hoc reporting on material incidents, breaches and risk profile changes.
Risk Committee	Oversees crypto risk framework implementation, reviews risk assessments, approves risk treatments, reviews KRIs, tracks remediation, evaluates emerging risks and recommends Board decisions.
Executive Management / COO	Ensures operations are resourced, compliant and aligned to approved risk appetite. Ensures crypto processes are operationally viable, customer-facing controls are implemented and escalation pathways are effective.
CFO / Finance & Treasury	Owns treasury exposure, fiat conversion, exchange/custodian balances, accounting, valuation, liquidity, reconciliation, concentration limits and financial reporting for digital assets.
Chief Risk Officer / Risk Function	Maintains the risk framework, methodology, risk register, appetite metrics, risk acceptance records and management reporting. Challenges business proposals and control performance.
Chief Compliance Officer / MLRO	Owns AML/CFT/CPF, sanctions, Travel Rule implementation, suspicious activity reporting, regulatory monitoring, customer risk escalation, CDD/EDD standards and regulator interaction.
Chief Information Security Officer	Owns wallet security standards, key management security, identity and access controls, vulnerability management, security monitoring, incident response and technology resilience.
Legal	Assesses regulatory perimeter, licence conditions, customer terms, vendor contracts, data sharing, law enforcement/regulator requests and cross-border implications.
Product / Payments / Operations	Owns day-to-day execution of approved crypto payment flows, transaction queues, holds, customer communication, operational procedures, staff training and incident detection.
Internal Audit / Independent Assurance	Tests design and operating effectiveness of this policy, crypto controls, third-party reliance, reconciliations, investigations, incident evidence and remediation closure.

3.2 Three lines of defence

The first line owns and operates controls in product, payments, operations, treasury and technology. The second line establishes standards and challenges performance through Risk, Compliance, Legal and Information Security. The third line provides independent assurance. The Company must maintain evidence that crypto controls are performed, exceptions are escalated and remediation is tracked to closure.

Line	Functions	Minimum responsibilities
First line	Payments, Operations, Product, Treasury, Technology	Execute approved procedures; perform transaction holds and releases; maintain reconciliations; complete checklists; evidence approvals; detect unusual activity; report incidents and breaches promptly.
Second line	Risk, Compliance, MLRO, Legal, CISO	Set policy and control standards; review risk assessments; approve high-risk exceptions; monitor KRIs; perform quality assurance; escalate to committee; manage regulatory interpretation.
Third line	Internal Audit / external assurance	Independently test governance, controls, evidence, system access, wallet security, vendor reliance, regulatory reporting and remediation effectiveness.

3.3 Delegated authorities and segregation of duties

Crypto transactions are irreversible and create heightened fraud, cyber, AML and operational risk. The Company must therefore maintain segregation between request, approval, execution, reconciliation and monitoring activities. A person who initiates a treasury transfer may not be the sole approver or reconciler. Wallet signatories must represent separate functions, and no private key holder may approve changes to his or her own access.

All delegated authorities must be documented in an authority matrix approved by the Risk Committee. Any emergency deviation from the authority matrix must be approved by at least two senior officers, logged in the policy exception register and reviewed at the next Risk Committee meeting.

4. Risk Appetite and Tolerance Limits

The Company maintains a low-to-moderate risk appetite for cryptocurrency activity. The Company is prepared to accept controlled crypto payment risk where it supports legitimate customer payment choice and business strategy, but it has no appetite for activity that compromises licensing, facilitates money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, customer harm, private key compromise or unapproved speculation.

Risk domain	Appetite	Mandatory tolerance statement
Regulatory / licensing	Low	No crypto activity may be launched or continued where Legal or Compliance concludes that required licence, registration, notification, contractual or regulator approval is absent.
AML/CFT/CPF	Low	No relationship or transaction may proceed where customer identity cannot be verified to the required standard, source of funds cannot be reasonably understood for the risk level, or suspicious activity cannot be mitigated.
Sanctions	Zero tolerance	No transaction, customer, beneficial owner, wallet, counterparty, jurisdiction or asset with confirmed sanctions nexus may be accepted, processed, returned, converted or released without MLRO and Legal approval consistent with applicable law.
Market / treasury	Low-to-moderate	Digital asset holdings must remain within approved exposure, concentration, liquidity and conversion limits. Speculative trading, leverage, margin, lending, staking and yield generation are prohibited unless separately approved by the Board.
Cyber / private key	Low	No single person may unilaterally move Company crypto assets. Private keys and signing authority must be protected by MFA, hardware-backed or MPC/HSM controls, segregation, logging and tested recovery arrangements.
Third party / outsourcing	Low-to-moderate	Only approved PSPs, custodians, exchanges, analytics and Travel Rule providers may be used. High residual vendor risk requires Risk Committee approval and documented compensating controls.
Operational	Low-to-moderate	Operational error risk must be reduced by maker-checker controls, whitelisted addresses, transaction simulations where relevant, chain/network validation and daily reconciliation.
Reputational	Low	The Company will not support assets, counterparties, jurisdictions or payment flows likely to cause serious reputational harm, customer detriment or regulator concern.

4.1 Quantitative limits

Unless a stricter limit is approved by the Board or imposed by law, the following limits apply. The Risk Committee may set lower limits by asset, customer segment, provider or jurisdiction based on risk conditions.

Limit area	Default limit	Control owner	Escalation trigger
Hot wallet exposure	Lesser of 5% of total crypto holdings or 7 days of average customer withdrawal volume.	CFO / CISO	Breach, failed sweep, unusual withdrawal spike or unplanned balance build-up.
Cold / qualified custody allocation	At least 95% of retained crypto holdings must be in approved cold, MPC/HSM or qualified custodian arrangements.	CFO / CISO	Any reduction below minimum without pre-approved operational rationale.
Total corporate crypto exposure	Not more than 10% of the trailing 30-day average gross gaming revenue equivalent, unless Board approved.	CFO	Exposure breach, high volatility, liquidity stress or material market event.
Single asset concentration	No single volatile crypto asset may exceed 35% of retained crypto holdings. Stablecoin concentration limits are set by issuer/custodian risk rating.	Treasury	Price shock, de-peg, issuer adverse news, exchange suspension.
Fiat conversion SLA	Customer deposit crypto intended for settlement should be converted to fiat or approved stable value asset within 24 hours where operationally and commercially feasible.	Treasury / Payments	Conversion backlog, market closure, provider outage or slippage > approved tolerance.

Limit area	Default limit	Control owner	Escalation trigger
Manual review queue	High-risk crypto alerts must be triaged within 4 business hours; potential sanctions or terrorist financing alerts immediately.	Compliance / MLRO	Aged alerts, backlog growth or missed regulatory reporting deadline.
Reconciliation breaks	Daily wallet, provider and ledger reconciliation must be completed by the next business day; unresolved breaks over 2 business days require escalation.	Finance	Unexplained balance difference, unsupported chain deposit, duplicate credit or missing transaction.

4.2 Prohibited activity

The following activities are prohibited unless the Board expressly approves a documented business case, legal analysis and risk treatment plan: proprietary speculative trading; use of margin, leverage, derivatives, lending, staking or yield strategies; direct use of mixers, tumblers, privacy-enhancing services or obfuscation protocols; acceptance of privacy coins or anonymity-enhanced assets; unsupported chains, wrapped assets or bridged assets without a risk assessment; processing transactions involving sanctioned persons, sanctioned jurisdictions or sanctioned wallet addresses; and any arrangement designed to conceal beneficial ownership, evade source-of-funds controls or bypass responsible gaming restrictions.

5. Crypto Risk Management Framework

The Company shall manage crypto risk using a documented lifecycle: identify, assess, control, monitor, report and improve. Risk assessments must cover inherent risk, control effectiveness, residual risk and risk treatment. Risk ownership must be assigned at the level capable of implementing the treatment plan. Residual high or critical risks must not be accepted informally.

5.1 Risk assessment methodology

Step	Requirement	Evidence
Identify	Identify crypto risks arising from customers, geographies, assets, blockchains, wallet architecture, payment channels, vendors, counterparties, employees, technology, regulation and incidents.	Risk register entry; process map; product approval form; vendor due diligence file.
Assess inherent risk	Score likelihood and impact before controls using the Company's 1-5 scale. Consider financial loss, regulatory exposure, customer harm, cyber compromise, operational disruption, liquidity, reputational impact and legal consequences.	Risk assessment worksheet; rationale for scoring; supporting data and typologies.
Evaluate controls	Assess preventive, detective and corrective controls for design adequacy and operating effectiveness. Consider automation, coverage, independence, timeliness, evidence quality and historical failures.	Control library; QA results; audit findings; system reports; access reviews.
Determine residual risk	Calculate residual risk after controls and classify as Low, Medium, High or Critical. Determine whether residual risk is within appetite.	Residual risk score; risk appetite mapping; management sign-off.
Treat risk	Choose avoid, reduce, transfer/share or accept. High and critical risks require documented remediation plans, owners, due dates and approval at the required level.	Risk treatment plan; action tracker; issue closure evidence.
Monitor and report	Track KRIs, incidents, breaches, exceptions, provider performance, regulatory change and risk trends. Escalate deterioration promptly.	Monthly dashboard; committee minutes; breach logs; KRI commentary.
Review and improve	Perform post-incident reviews, annual control testing and policy review. Update controls after typology, regulation, technology or business changes.	Lessons learned; audit reports; updated procedures; revised policy.

5.2 Risk scoring

Likelihood and impact must be scored on a 1 to 5 basis. Risk assessments must not average away a severe regulatory, sanctions, cyber or customer harm impact. A low likelihood but catastrophic impact scenario may still require high residual risk classification and senior approval.

Score	Likelihood guidance	Impact guidance
-------	---------------------	-----------------

Score	Likelihood guidance	Impact guidance
1 - Rare / Minimal	Unlikely in normal operations and no known history.	Limited process inconvenience, no customer harm, no reportable issue, negligible financial loss.
2 - Unlikely / Minor	Possible but not expected; isolated event.	Minor remediation, limited financial impact, no material regulator or customer effect.
3 - Possible / Moderate	Could occur under realistic conditions or has occurred in the sector.	Customer complaints, control breach, investigation backlog, moderate loss, management attention required.
4 - Likely / Major	Expected periodically or known recurring sector typology.	Regulatory notification likely, significant loss, material customer impact, service disruption or reputational concern.
5 - Almost certain / Severe	Expected frequently without strong controls or currently occurring.	Licence threat, sanctions breach, major cyber loss, systemic AML failure, severe customer harm or existential reputational impact.

5.3 Risk taxonomy

Risk category	Description	Core controls	Primary owner
Regulatory and licensing	Risk of breach of gaming, financial crime, VASP/CASP, data, consumer protection, advertising, tax or reporting obligations.	Regulatory change monitoring; legal reviews; licensing assessments; policy review; regulator engagement; jurisdictional restrictions.	Legal / Compliance
AML/CFT/CPF and fraud	Risk that crypto is used for laundering, terrorist financing, proliferation financing, fraud, scams, mule activity, stolen funds, ransomware, darknet activity or layering.	CDD/EDD; source-of-funds review; blockchain analytics; transaction monitoring; suspicious activity reporting; typology rules; responsible gaming coordination.	MLRO / Compliance
Sanctions	Risk of dealing with sanctioned persons, wallets, jurisdictions, exchanges, protocols or beneficial owners.	Real-time screening; list updates; wallet screening; holds/freezes; escalation; no tipping off; regulator/law enforcement reporting.	Compliance / MLRO
Market and liquidity	Risk from volatility, de-pegging, slippage, exchange illiquidity, conversion failure or concentration.	Approved asset register; exposure limits; conversion SLA; liquidity monitoring; stablecoin risk triggers; treasury reporting.	CFO / Treasury
Custody and private key	Risk of lost keys, unauthorized signing, wallet compromise, insider collusion, operational transfer error or custodian failure.	MPC/HSM/cold storage; multi-signature; maker-checker; whitelisting; key ceremonies; access reviews; recovery tests; segregation of duties.	CISO / CFO
Cybersecurity and technology	Risk of phishing, malware, API compromise, vulnerability exploitation, cloud misconfiguration, data leakage or monitoring failure.	MFA; PAM; SIEM; vulnerability management; secure SDLC; endpoint security; encryption; incident response; penetration testing.	CISO
Operational and process	Risk from human error, unsupported networks, duplicate credits, wrong-chain deposits, reconciliation failures or inadequate procedures.	SOPs; training; four-eyes controls; chain validation; reconciliation; exception handling; QA; process ownership.	COO / Operations
Third-party and outsourcing	Risk from PSPs, custodians, exchanges, analytics vendors, Travel Rule providers, cloud providers or banking partners.	Due diligence; contracts; SLAs; audit rights; concentration limits; ongoing monitoring; exit plans; incident notification clauses.	Vendor Owner / Risk
Data protection and confidentiality	Risk of misuse, over-retention, unauthorized disclosure or insecure transmission of customer, Travel Rule or investigation data.	Access controls; encryption; retention schedules; privacy impact assessments; secure data sharing; breach notification process.	DPO / Legal / CISO
Reputational and customer harm	Risk that crypto controls, incidents, customer complaints or public typologies damage trust or responsible gaming outcomes.	Customer disclosures; responsible gaming monitoring; incident communications; executive escalation; product risk review.	Executive Management

6. Regulatory Perimeter and Permitted Crypto Activities

Before any crypto activity is undertaken, the Company must determine whether the activity creates direct or indirect obligations as a gaming operator, money service business, VASP, CASP, payment institution, custodian, exchange, e-money issuer, issuer of crypto-assets, data controller, tax reporting entity or other regulated activity. The conclusion must be documented and approved by Legal and Compliance.

6.1 Permitted activity model

The Company's permitted model is limited to accepting approved digital assets as a customer payment channel for lawful gaming services, returning withdrawals to approved customer destinations, retaining only limited operational

liquidity, and using approved providers for conversion, settlement, analytics, Travel Rule handling and custody. Any activity outside this model requires a new product approval.

Activity	Policy status	Minimum approval
Customer crypto deposits for gaming wallet funding	Permitted only through approved flows, approved assets, CDD/EDD controls, blockchain analytics and transaction monitoring.	Payments, Compliance, MLRO and Risk.
Customer crypto withdrawals	Permitted only after account risk checks, sanctions/wallet screening, balance and responsible gaming checks, destination address validation and required Travel Rule controls.	Operations/Payments with Compliance escalation for alerts.
Treasury retention of crypto	Permitted within limits and only for operational liquidity or approved treasury reasons. Speculation prohibited.	CFO with Risk Committee oversight.
Third-party PSP/custodian/exchange use	Permitted only after vendor due diligence, contractual controls, security review and ongoing monitoring.	Vendor Owner, Risk, Legal, CISO, Compliance, CFO.
New token, chain, network or wallet integration	Prohibited until asset, legal, compliance, treasury, technology and operational risk assessments are approved.	Risk Committee or delegated authority.
DeFi, staking, lending, derivatives, margin, market making, token issuance	Prohibited unless separately approved by the Board under a dedicated policy and legal analysis.	Board approval required.

6.2 Jurisdictional restrictions

The Company shall maintain a Restricted Jurisdiction Register covering customer residence, nationality, IP location, geolocation, device indicators, payment origin, wallet exposure and counterparty location. Restricted jurisdiction rules must reflect licensing restrictions, sanctions, FATF/CFATF notices, local law, PSP/custodian restrictions and banking partner requirements. Customers must not be allowed to use crypto to bypass jurisdictional controls.

Where geolocation, VPN, proxy, device fingerprinting, KYC information, blockchain analytics or payment data suggests a restricted jurisdiction nexus, the transaction must be paused and escalated to Compliance. The Company must not rely solely on customer self-declaration where other indicators suggest a conflicting location or risk profile.

7. Digital Asset Approval and Product Risk Controls

Digital assets must not be accepted merely because a provider supports them. Each asset, network and settlement flow must be approved through a documented Digital Asset Risk Assessment. The assessment must consider regulatory status, liquidity, volatility, technology risk, illicit finance exposure, sanctions exposure, stablecoin issuer risk, operational supportability, custodian support, accounting impact and customer communication requirements.

7.1 Approved Digital Asset Register

The Company shall maintain an Approved Digital Asset Register. The register must identify the approved asset, supported network, permitted use, provider(s), minimum confirmations, conversion method, exposure limit, relevant wallet type, risk rating, review date and owner. Any asset not listed in the register is prohibited.

Criterion	Minimum considerations
Legal and regulatory	Is the asset a crypto-asset, e-money token, asset-referenced token, financial instrument, security, commodity, stablecoin or otherwise regulated product in relevant jurisdictions? Are customer disclosures or licensing obligations triggered?
AML/sanctions risk	What illicit finance typologies, darknet exposure, mixer usage, ransomware exposure, sanctions designations, chain-hopping risks or privacy features are associated with the asset or network?
Market risk	Does the asset have sufficient liquidity, reliable price feeds, limited slippage, credible market depth and acceptable volatility for customer deposits and withdrawals?
Technology and protocol risk	Is the network operationally stable? Are there risks from forks, smart contracts, bridge dependencies, validator centralization, finality, congestion or unsupported token standards?
Custody and operations	Can the asset be securely supported by approved custodians, wallets, analytics tools and finance systems? Are deposits/withdrawals reversible? Can unsupported network deposits be handled?
Stablecoin-specific risk	If a stablecoin, does it have credible reserves, redemption arrangements, regulatory standing, transparency reports, issuer risk controls and de-peg monitoring?
Customer communication	Are customer disclosures clear on supported networks, confirmations, fees, volatility, irreversibility, potential holds, unsupported transfers and withdrawal requirements?

7.2 Prohibited and restricted asset features

Assets with anonymity-enhancing features, built-in mixing, insufficient transaction traceability, unsupported analytics coverage, sanctioned protocol exposure, extreme volatility, inadequate liquidity, severe de-peg history, unverified smart contracts, misleading customer disclosures or inadequate custody support shall not be approved. Bridged, wrapped or synthetic assets require specific approval because bridge risk, issuer risk and redemption risk can differ materially from the underlying asset.

7.3 Product change management

Any change to a crypto customer journey, wallet infrastructure, PSP routing, custody model, transaction monitoring rule, supported asset, supported network, settlement currency or withdrawal process must follow controlled change management. The change must include risk assessment, security review, test results, rollback plan, customer impact analysis, training updates, procedure updates and go-live approval. Emergency changes must be logged and retrospectively approved within five business days.

8. Customer, Wallet and Transaction Risk Management

Customer risk management is central to crypto safety. The Company must identify customers to the required standard, understand expected account activity, monitor wallet behaviour, identify unusual patterns, apply risk-based limits and escalate activity that may indicate fraud, money laundering, terrorist financing, sanctions evasion, responsible gaming harm or policy circumvention.

8.1 Customer due diligence and risk classification

Customer due diligence must be completed in accordance with the Company's AML/CFT/CPF and Customer Due Diligence policies. Crypto activity must not be treated as low risk solely because blockchain data is transparent. Customer identity, location, source of funds, source of wealth where applicable, wallet ownership and activity profile must be assessed together.

Risk tier	Indicative criteria	Required treatment
Low	Identity verified; customer is in an allowed jurisdiction; expected activity is modest and consistent; blockchain exposure is clean; no adverse media, sanctions, PEP or responsible gaming concern.	Standard CDD, automated monitoring, standard deposit/withdrawal limits and periodic review.
Medium	Higher transaction volume; multiple wallets; limited use of exchanges; activity inconsistent with declared profile; early warning blockchain exposure; repeated rapid deposits/withdrawals; device or location anomalies.	Enhanced monitoring, documented rationale for continued relationship, possible source-of-funds request, reduced limits or manual review for selected transactions.
High	High-risk jurisdiction nexus; PEP; adverse media; complex wallet activity; use of high-risk exchanges, bridges or P2P services; material source-of-funds uncertainty; frequent account cycling; responsible gaming red flags.	EDD, source-of-funds/source-of-wealth review, senior Compliance approval, transaction holds as needed, enhanced ongoing monitoring and documented review cycle.
Prohibited / exit	Confirmed sanctions match, terrorist financing indicator, direct mixer/tumbler interaction, darknet market exposure, stolen funds, confirmed fraud, impersonation, forged documentation, banned jurisdiction or refusal to provide required information.	Do not onboard or continue relationship; freeze or reject where required; escalate to MLRO/Legal; report to FIU/regulator/law enforcement where applicable; avoid tipping off.

8.2 Wallet attribution and ownership

The Company shall maintain a risk-based approach to wallet ownership. For lower-risk customers and low-value transactions, blockchain analytics and customer declarations may be sufficient where permitted by law. For higher-risk or higher-value activity, the Company may require proof of control of the wallet, such as a signed message, micro-transfer, exchange account statement, screenshot supported by verification, or other method approved by Compliance and Information Security.

A customer must not be allowed to repeatedly change withdrawal addresses, route funds through unrelated third parties or withdraw to wallets inconsistent with the customer's risk profile without review. Third-party payments and

withdrawals are prohibited unless expressly approved by Compliance and supported by a documented legal and AML rationale.

8.3 Transaction monitoring controls

Crypto deposits and withdrawals must be screened before customer value is made available or before funds are broadcast, except where a documented technical constraint exists and compensating controls are approved. Monitoring must combine rules-based scenarios, blockchain analytics, customer profile information, geolocation/device data, payment history, responsible gaming indicators and manual investigation.

Control stage	Minimum requirement
Deposit address assignment	Assign addresses only through approved wallet infrastructure. Address generation must be logged, linked to the customer account and protected from tampering.
Pre-credit screening	Screen incoming transaction, source wallet, exposure path, asset, network, amount, sanctions indicators and typology red flags before crediting value whenever possible.
Confirmations and finality	Credit deposits only after the minimum confirmations in the Approved Digital Asset Register, adjusted for network congestion, reorg risk and asset-specific finality risk.
Withdrawal screening	Screen destination wallet, customer account status, responsible gaming holds, sanctions exposure, Travel Rule requirements, prior fraud flags and velocity rules before release.
Velocity and behavioural rules	Identify rapid in/out with little or no gameplay, structured deposits, dormant account reactivation, multiple wallets, round-number transactions, use of VPN/proxies, high-risk exchange exposure and unusual chain-hopping.
Case management	Alerts must be triaged, assigned, investigated, documented, resolved and subject to quality assurance. Decisions to release, reject, freeze, return or report must be evidence-based.

8.4 Red flag indicators

The following red flags must be incorporated into transaction monitoring and investigation procedures. They are not exhaustive; staff must escalate any activity that appears inconsistent, suspicious, evasive or harmful even where no automated rule is triggered.

Type	Examples
Customer behaviour	Customer refuses or delays required KYC/EDD; uses inconsistent identity/location information; changes wallet addresses frequently; uses multiple accounts; requests urgent withdrawal after deposit; deposits and withdraws without meaningful gameplay; uses VPN/proxy or device patterns inconsistent with declared residence.
Wallet and blockchain	Direct or indirect exposure to sanctioned wallets, darknet markets, mixers/tumblers, ransomware wallets, stolen funds, scams, high-risk exchanges, unlicensed services, nested services, bridges used for obfuscation, peel chains or chain-hopping patterns.
Transaction pattern	Structuring just below thresholds; unusually high velocity; round-number transactions; multiple deposits from unrelated wallets; withdrawals to multiple new addresses; rapid conversion across assets; activity inconsistent with customer income or declared source of funds.
Responsible gaming overlap	Escalating deposits, chasing losses, rapid crypto top-ups after card/bank limits, requests to bypass limits, signs of distress or use of crypto to avoid responsible gaming controls.

9. AML/CFT/CPF, Sanctions and Travel Rule Controls

The Company shall maintain AML/CFT/CPF controls that are appropriate to the risks of cryptocurrency and gaming. Crypto controls must be integrated with the Company's wider financial crime framework, not operated in isolation. The MLRO has authority to pause, reject, freeze, report or exit activity where required to manage financial crime risk.

9.1 AML/CFT/CPF control standards

CDD, EDD, transaction monitoring, source-of-funds checks, suspicious activity reporting and ongoing monitoring must be risk-based and evidenced. The Company must be able to demonstrate why a customer, wallet, transaction or provider was considered acceptable. The inability to obtain reasonable information for the risk presented is itself a risk factor and may justify rejection or exit.

Control	Requirement
---------	-------------

Control	Requirement
CDD	Identify and verify customers before crypto activity where required by law or risk; screen sanctions/PEP/adverse media; verify location and age; apply responsible gaming controls.
EDD	Perform enhanced review for high-risk customers, PEPs, high-risk jurisdictions, complex wallet activity, large volumes, adverse media, source-of-funds uncertainty or unusual behaviour.
Source of funds/source of wealth	Request evidence such as exchange statements, transaction history, employment/business income, asset sale evidence, wallet history, bank statements or other reliable information appropriate to risk.
Ongoing monitoring	Review customer profile, transaction patterns, wallet exposure, risk triggers, alerts, responsible gaming indicators and new adverse information throughout the relationship.
Suspicious activity reporting	Escalate potential unusual or suspicious activity to the MLRO. File reports to FIU Curaçao or other applicable authority where required. Maintain confidentiality and avoid tipping off.
Quality assurance	Compliance must perform periodic QA over alerts, EDD, source-of-funds decisions, SAR/UTR decisions, sanctions screening and case closure rationale.

9.2 Sanctions controls

The Company has zero tolerance for sanctions breaches. Sanctions screening must cover customers, beneficial owners, directors, authorized users, wallets, counterparties, vendors, jurisdictions, IP/device indicators, PSPs, custodians, exchanges, smart contract/protocol exposure and blockchain transaction exposure. Screening must occur at onboarding, before relevant transactions, during ongoing monitoring, when lists change and when adverse intelligence is received.

Potential sanctions matches must be escalated immediately to the MLRO and Legal. Funds must not be returned, converted, released or moved solely to resolve operational inconvenience. The Company must assess legal freeze, blocking, reporting and notification obligations and must not tip off customers or counterparties. False-positive decisions must be documented with evidence.

9.3 Travel Rule and counterparty VASP/CASP due diligence

Where the Company directly or indirectly performs, instructs or controls crypto transfers that fall within Travel Rule or VASP/CASP obligations, it must ensure that required originator and beneficiary information is obtained, verified as required, transmitted securely, retained and made available to competent authorities where legally required. Where a PSP, custodian or CASP performs this function, the Company must assess the provider's capability, contractual obligations, data security and control evidence.

Area	Policy requirement
Required information	Collect, transmit and retain originator and beneficiary information required by applicable law or provider obligations. Information must be accurate, timely and securely transmitted.
Counterparty identification	Determine whether the transfer involves another VASP/CASP, financial institution, unhosted wallet or other counterparty. Use reliable registries, provider data, blockchain analytics and due diligence.
Counterparty due diligence	Assess counterparty VASP/CASP licensing, ownership, jurisdiction, AML/sanctions controls, Travel Rule capability, data protection, reputation, enforcement history and willingness to provide required information.
Missing or incomplete information	Establish rules to reject, hold, suspend, request information or escalate transfers lacking required information. Repeat deficiencies by a counterparty must be reviewed for relationship restrictions.
Unhosted wallets	Apply risk-based wallet ownership verification, transaction limits, enhanced monitoring and escalation. Higher-risk unhosted wallet activity requires Compliance review.
Data protection	Travel Rule data must be shared only through secure, approved channels with lawful basis, access controls, retention limits and confidentiality protections.

9.4 Suspicious activity handling

When activity appears unusual or suspicious, Operations must not resolve the matter through customer service alone. The case must be escalated to Compliance/MLRO with relevant customer, wallet, blockchain, device, geolocation, transaction and communications data. The MLRO determines whether to continue monitoring, request information, restrict account activity, reject or return funds where lawful, freeze funds, file a report, notify regulators or exit the relationship.

10. Wallet, Custody and Private Key Risk Management

Wallet and private key controls are critical because crypto transactions can be irreversible and key compromise can lead to immediate loss. The Company shall use secure, auditable and segregated wallet arrangements. Direct self-custody must be approved by the Risk Committee and CISO; otherwise, customer-facing crypto payment flows should use approved PSPs and custodians with evidence of security, compliance and resilience.

10.1 Wallet architecture

Wallet / custody type	Purpose	Control requirements
Hot wallet	Limited daily operational liquidity and customer withdrawal processing.	Balance capped by appetite; automated alerts; strict withdrawal limits; MFA/PAM; API key restrictions; no long-term storage; daily sweeps; real-time monitoring.
Warm wallet / operational custody	Intermediate operational balances, provider settlement, controlled liquidity buffer.	Multi-approval transfers; restricted access; whitelisted destinations; periodic sweeps; monitoring; reconciliation.
Cold storage / qualified custody	Longer-term retained holdings and treasury reserves.	Offline/MPC/HSM/custodian controls; multi-signature; key ceremony; geographically separate backups; recovery testing; limited signers; insurance/assurance where available.
Third-party PSP / custodian wallet	Customer deposit/withdrawal processing, conversion and settlement.	Vendor due diligence; contractual SLAs; segregation; reporting; incident notification; audit rights; proof of control/ownership where applicable.

10.2 Private key and signing controls

Private keys, recovery phrases, MPC shares, HSM credentials, API keys and signing devices must be generated, stored, used, rotated, backed up and destroyed under documented key management procedures. Key material must never be stored in plaintext, shared through messaging applications, photographed, emailed, copied to unmanaged devices or accessible to a single employee without compensating controls.

Control area	Mandatory requirement
Key generation	Generate keys or MPC shares in a controlled ceremony with two or more authorised persons, recorded checklist, tamper-evident materials and CISO or delegate oversight.
Storage	Store key material or recovery components in approved secure facilities, HSM/MPC infrastructure or safes with access logs, dual control and environmental protections.
Signing approvals	Use at least 2-of-3 approval for low-value operational transfers and 3-of-5 for material treasury/cold storage transfers unless a stricter matrix applies. Signers must be from separate functions.
Access management	Grant least-privilege access, require MFA/hardware keys, prohibit shared accounts, review access quarterly and immediately revoke access on role change or termination.
Whitelisting	Treasury, custodian, exchange and PSP destination addresses must be pre-approved, verified out-of-band, locked where technically possible and subject to change controls.
Backups and recovery	Maintain tested recovery procedures. Recovery tests must not expose production keys and must be witnessed, logged and reviewed by CISO and Risk.
Rotation and compromise	Rotate or disable credentials after suspected compromise, staff departure, vendor compromise, control failure or as required by key management standards.

10.3 Transaction execution controls

All material crypto transfers must be supported by a transaction ticket specifying business purpose, asset, network, amount, fiat equivalent, source wallet, destination wallet, counterparty, approvals, screening result, Travel Rule status, expected fees and reconciliation reference. Maker-checker approval must occur before broadcast. Address and network must be verified through approved tooling and out-of-band procedures where the transfer is material or new.

Transaction type	Minimum approval	Additional controls
Customer withdrawal within automated risk limits	Automated controls plus operations monitoring; escalation for alerts.	Sanctions/wallet screening, customer status check, responsible gaming hold check, Travel Rule where applicable.
Manual customer withdrawal override	Operations manager plus Compliance approval.	Case note, rationale, customer communication record, post-release reconciliation.

Transaction type	Minimum approval	Additional controls
Hot wallet refill/sweep	Treasury plus Security/Operations approval.	Whitelisted addresses, balance limits, reconciliation, alerting.
Cold storage / custodian transfer	3-of-5 signers including Finance, Security and Risk/Compliance or delegated senior officer.	Transaction ticket, out-of-band address verification, pre-broadcast screen, post-broadcast verification, committee notification for material amount.
Provider/exchange transfer	CFO/Treasury plus Compliance if counterparty or jurisdiction risk is elevated.	Provider status check, exchange/custodian limit check, market/liquidity assessment, Travel Rule/data checks.

10.4 Reconciliation and proof of balances

Finance must reconcile wallet, provider, blockchain and general ledger records daily for operational wallets and at least monthly for cold/custody balances, or more frequently where balances are material. Reconciliations must identify pending transactions, chain fees, failed transactions, deposits not credited, withdrawals not broadcast, duplicate credits, unsupported network transfers and provider balance differences. Material unexplained breaks must be escalated to CFO, Risk and Compliance.

11. Treasury, Market, Liquidity and Stablecoin Risk Management

The Company does not maintain crypto holdings for speculative investment. Digital assets may be retained only for approved operational liquidity, customer settlement, treasury reserve purpose approved by the CFO/Risk Committee, or as required by provider mechanics. Exposure must be measurable, monitored and within appetite.

11.1 Market risk controls

Treasury must monitor price volatility, liquidity, exchange availability, slippage, conversion capacity, provider downtime, market disruption, stablecoin de-pegging, asset concentration and settlement delays. Where price volatility or liquidity stress threatens appetite limits or customer settlement, Treasury must execute the approved market disruption playbook and inform the Risk Committee.

Risk	Control standard
Volatility	Use automated or scheduled conversion to fiat or approved stable value asset within the conversion SLA. Monitor exposure against approved limit at least daily.
Slippage and liquidity	Use approved venues/providers with sufficient market depth. Escalate slippage above tolerance and suspend assets where fair conversion is not available.
Stablecoin de-peg	Monitor price, redemption, reserve, issuer, chain and exchange indicators. Escalate if de-peg exceeds 2% for more than one hour, redemptions are suspended, or credible adverse news emerges.
Exchange / custodian concentration	Maintain exposure limits by provider, consider creditworthiness and operational resilience, and avoid keeping excess balances on exchanges.
Settlement delay	Track fiat off-ramp delays and banking disruptions. Maintain alternative approved providers or contingency liquidity where material.
Fees and network congestion	Monitor transaction fees, congestion and confirmation delays. Adjust customer disclosures and operational limits when network conditions are stressed.

11.2 Treasury prohibitions and approvals

Treasury may not use Company assets for margin, leverage, derivatives, staking, lending, yield products, liquidity mining, structured products, proprietary day trading or speculative rebalancing. Hedging may be considered only where it reduces risk, is legally permissible, uses approved counterparties, is documented under a Board-approved strategy and is independently monitored.

11.3 Accounting and valuation

Finance must maintain accounting records that identify transaction date/time, blockchain transaction hash, asset, quantity, fiat value at recognition, fees, settlement value, custodian/provider reference, customer account reference and realised gain/loss or expense treatment where applicable. Valuation sources must be approved, consistent and

independently reviewable. Finance must assess tax, financial reporting and audit implications before new assets or settlement models are introduced.

12. Cybersecurity, Technology and Operational Resilience

Crypto activity increases the consequences of cyber control failure. The Company shall implement security controls for wallet infrastructure, APIs, employee access, vendor connectivity, customer-facing payment journeys, logs, monitoring, data transmission and incident response. Cyber controls must align to enterprise risk governance and the NIST CSF functions of Govern, Identify, Protect, Detect, Respond and Recover.

12.1 Minimum cybersecurity controls

Domain	Minimum control requirements
Govern	Document ownership, risk appetite, policies, supplier responsibilities, architecture approvals, security exceptions and executive reporting.
Identify	Maintain inventory of wallets, keys, APIs, providers, cloud resources, secrets, privileged accounts, data flows and critical crypto processes.
Protect	Use MFA/hardware keys, PAM, least privilege, encryption, secret management, network segmentation, secure configuration, endpoint protection, secure SDLC and staff training.
Detect	Log wallet, provider, admin, API and transaction events. Monitor SIEM alerts, unusual access, key/signing events, blockchain alerts, provider status and anomalous customer/payment behaviour.
Respond	Maintain crypto incident playbooks for wallet compromise, unauthorized transfer, sanctions hit, ransomware, provider outage, Travel Rule failure, data breach and market disruption.
Recover	Maintain tested backups, wallet recovery, provider failover, communication plans, reconciliation recovery and lessons-learned actions.

12.2 Secure development and change controls

Any code, API integration, webhook, wallet address generator, transaction monitoring rule, customer-facing crypto payment page, data pipeline or reconciliation process must be developed and changed under secure SDLC and change management controls. Testing must include negative scenarios, unsupported networks, duplicate callbacks, delayed confirmations, chain reorgs, provider outage, replayed webhooks, address tampering, sanctions alerts and reconciliation breaks.

12.3 Business continuity and resilience

Business continuity plans must address the unavailability of crypto PSPs, exchanges, custodians, blockchain networks, analytics providers, Travel Rule providers, banking partners, cloud services and internal payment systems. Continuity plans must define customer communications, transaction holds, alternative processing, settlement delays, manual review, risk acceptance and recovery priorities. Plans must be tested at least annually and after material architecture changes.

13. Third-Party, Custodian and Crypto Payment Provider Risk

The Company may rely on third parties for payment processing, custody, conversion, analytics, Travel Rule messaging, blockchain data, cloud infrastructure and incident support. These arrangements must be governed through the Vendor Risk Management Policy and crypto-specific due diligence. A provider must not be onboarded solely on commercial grounds.

13.1 Due diligence

Due diligence area	Minimum review requirement
Regulatory status	Verify licences, registrations, supervisory status, jurisdiction, authorised activities, enforcement history and ability to serve the Company's customer base.
Ownership and reputation	Review ownership, beneficial owners, management, adverse media, sanctions, litigation, insolvency concerns and market reputation.
AML/sanctions/Travel Rule	Assess CDD, transaction monitoring, sanctions screening, Travel Rule capabilities, case management, suspicious reporting support and audit evidence.

Due diligence area	Minimum review requirement
Custody and security	Review key management, MPC/HSM/cold storage, segregation, insurance, SOC/ISO reports, penetration testing, vulnerability management, incident history and access controls.
Financial resilience	Review financial statements where available, proof-of-reserves or assurance reports, capital/liquidity indicators, concentration and banking/off-ramp arrangements.
Operational resilience	Assess uptime, SLAs, disaster recovery, support model, incident notification, reconciliation files, transaction limits, settlement times and customer impact procedures.
Data protection	Review data processing terms, confidentiality, encryption, location of processing, sub-processors, retention, breach notification and Travel Rule data safeguards.
Exit and contingency	Define data portability, wallet migration, asset withdrawal, termination rights, transition plan, escrow/backup options and continuity arrangements.

13.2 Contractual controls

Contracts with crypto providers must include, where applicable, scope of services, compliance warranties, service levels, incident notification timelines, regulator and audit cooperation, confidentiality, data protection, sanctions and AML obligations, Travel Rule obligations, segregation/safeguarding terms, reconciliation reporting, termination rights, business continuity commitments, subcontractor controls, liability provisions and the right to suspend services when required by law or risk appetite.

13.3 Ongoing monitoring

Provider performance and risk profile must be reviewed at onboarding, annually and upon trigger events such as regulatory action, data breach, wallet loss, service outage, ownership change, deteriorating financial condition, sanctions exposure, adverse media, proof-of-reserves concern, major customer complaint or significant control failure. High-risk providers require enhanced monitoring and Risk Committee reporting.

14. Accounting, Recordkeeping, Data Protection and Evidence

The Company must maintain complete, accurate and retrievable records of crypto activity sufficient to evidence compliance with law, licence obligations, customer terms, financial reporting standards, audits, investigations and regulator requests. Records must be protected against unauthorized access, alteration, deletion and inappropriate disclosure.

14.1 Minimum records

Record type	Minimum retained content
Customer records	KYC/CDD/EDD, risk rating, jurisdiction checks, PEP/sanctions/adverse media results, source-of-funds/source-of-wealth evidence, wallet ownership evidence and communications.
Transaction records	Date/time, asset, amount, fiat value, wallet addresses, transaction hash, confirmations, fees, customer account, provider reference, screening results, Travel Rule data and settlement status.
Case records	Alert details, investigation notes, blockchain analytics evidence, screenshots/reports, decision rationale, approvals, SAR/UTR filing decision, restrictions and closure evidence.
Wallet/custody records	Address inventory, key ceremony records, signer lists, access reviews, transaction tickets, approvals, reconciliation, provider/custodian statements and recovery tests.
Provider records	Due diligence, approvals, contracts, audit reports, SOC/ISO reports, SLAs, incidents, periodic reviews, exit plans and remediation.
Governance records	Risk assessments, risk register, appetite approvals, committee minutes, KRIs, breaches, exceptions, training, audits, policy review and remediation trackers.

14.2 Retention and privacy

Crypto records must be retained for at least five years after the end of the customer relationship or transaction, or longer where required by Curaçao law, regulator request, litigation hold, tax rules, licence conditions, applicable data protection law or contractual obligations. Travel Rule and investigation data must be retained securely and shared only with authorised parties for lawful purposes.

The Company shall apply privacy-by-design and data minimisation. Access to customer, Travel Rule and investigation data must be restricted to authorised personnel with a business need. Data transfers to providers or counterparties must use approved secure channels and be covered by appropriate contractual and legal safeguards.

15. Incident Management, Escalation and Crisis Response

Crypto incidents can escalate quickly and may require immediate containment, regulatory reporting, customer communication, provider coordination and law enforcement engagement. The Company shall maintain crypto-specific incident playbooks integrated with the enterprise Incident Response Plan and Business Continuity Plan.

15.1 Incident types

Category	Examples
Security	Wallet compromise, unauthorized signing, lost key share, phishing of a signer, malware, API key compromise, data breach, ransomware, suspicious admin access.
Financial crime	Confirmed sanctions hit, terrorist financing indicator, ransomware funds, mixer/darknet exposure, suspicious transaction pattern, suspected fraud, mule activity, stolen funds.
Operational	Wrong-chain transfer, duplicate credit, unsupported network deposit, provider webhook failure, reconciliation break, delayed confirmations, transaction broadcast error.
Market / treasury	Stablecoin de-peg, exchange/custodian suspension, fiat off-ramp failure, extreme volatility, provider insolvency signal, liquidity freeze.
Regulatory / reporting	Missed reporting deadline, regulator inquiry, Travel Rule failure, licence condition breach, provider non-compliance affecting the Company.
Customer impact	Material withdrawal delay, incorrect customer balance, customer data exposure, customer harm linked to crypto controls or responsible gaming failure.

15.2 Escalation timeline

Any employee, contractor or provider who becomes aware of a crypto incident or suspected incident must report it immediately through the approved incident channel. Potential sanctions, terrorist financing, wallet compromise, unauthorized transfer or data breach events must be escalated without delay, regardless of value.

Severity	Trigger examples	Initial escalation	Management reporting
Critical	Confirmed wallet compromise; material loss; sanctions breach; terrorist financing; major data breach; custodian insolvency affecting assets; licence-threatening failure.	Immediately and no later than 30 minutes to CISO, MLRO, CFO, CRO, COO and Legal.	CEO/Board within 24 hours; regulator/FIU/law enforcement notifications as legally required.
High	Suspected compromise; significant transaction monitoring failure; high-value wrong transfer; major provider outage; stablecoin de-peg; material reconciliation break.	Within 1 hour to relevant control owners and incident manager.	Risk Committee chair within 24 hours; regulator assessment documented.
Medium	Limited operational error; isolated delayed withdrawal; non-material provider issue; alert backlog above tolerance.	Same business day to process owner and Compliance/Risk if applicable.	Monthly incident reporting with remediation actions.
Low	Minor issue with no customer, regulatory or financial impact and immediate correction.	Log in incident/issue register.	Trend reporting through monthly management information.

15.3 Incident response process

The incident response process must include triage, severity classification, containment, preservation of evidence, legal privilege assessment where applicable, blockchain tracing, provider coordination, customer impact assessment, regulatory reporting assessment, communications approval, recovery, reconciliation, root-cause analysis, remediation and lessons learned. Movement of potentially tainted or sanctioned assets must not occur without MLRO and Legal approval.

Following any High or Critical crypto incident, the Risk Committee must receive a post-incident report covering timeline, root cause, impacted customers/assets, control failures, financial and regulatory impact, decisions taken, reporting completed, remediation owners, due dates and assurance plan. Remediation must be tracked to closure and independently verified where material.

16. Monitoring, Reporting, KRIs and Management Information

Management information must allow the Board, Risk Committee and control functions to understand the crypto risk profile, control effectiveness, breaches, emerging threats, customer impact and remediation status. Reporting must be accurate, timely, risk-based and supported by source evidence.

16.1 Reporting schedule

Frequency	Report	Owner	Audience
Daily	Wallet balance, hot wallet exposure, conversion status, material alerts, reconciliation breaks, provider outage, high-risk transaction queue.	Treasury / Operations / Compliance	CFO, COO, MLRO, CISO as relevant.
Weekly	Financial crime alert trends, aged cases, high-risk customers, withdrawal holds, sanctions false positives, provider exceptions.	Compliance / MLRO	Compliance leadership, Operations, Risk.
Monthly	Crypto Risk Dashboard covering exposure, transactions, customer risk, KRIs, incidents, breaches, vendor performance, audit actions and regulatory change.	Risk Function	Executive Management and Risk Committee.
Quarterly	Risk appetite review, risk register update, vendor risk review, wallet security review, customer risk trends, control testing results and strategic recommendations.	CRO / CCO / CISO / CFO	Risk Committee and Board.
Annually	Crypto enterprise risk assessment, policy review, independent audit/assurance, penetration test summary, business continuity test and training completion.	Risk / Internal Audit / CISO	Board / Risk Committee.
Ad hoc	High or Critical incidents, sanctions matches, regulator inquiries, material market events, provider insolvency, critical control failure or appetite breach.	Relevant owner	CEO, Board/Risk Committee, Legal, regulators as required.

16.2 Key Risk Indicators

KRI	Target / threshold	Escalation
Hot wallet balance as percentage of total holdings	<= 5% or approved operational threshold	CFO/CISO if breached; Risk Committee if unresolved.
Crypto exposure versus approved limit	<= approved exposure and concentration limits	CFO and Risk for breach; Board for material or repeated breach.
High-risk transaction alerts aged over SLA	0 critical; <= agreed tolerance for high/medium	MLRO and COO for backlog; Risk Committee for trend.
Confirmed or potential sanctions alerts	0 confirmed breaches	Immediate MLRO/Legal escalation and reporting assessment.
Unreconciled wallet/provider breaks	0 material unexplained breaks over 2 business days	CFO, Risk and Internal Audit if recurring.
CDD/EDD overdue for crypto-active customers	<= agreed tolerance; 0 high-risk overdue	Compliance leadership and Risk Committee.
Provider SLA breaches / outages	Within contract tolerance	Vendor owner and Risk; exit plan review for repeated failure.
Wallet security access review completion	100% quarterly completion	CISO; Risk Committee for missed cycle.
Policy exceptions open past due	0 past due High/Critical exceptions	CRO and Risk Committee.
Crypto incidents by severity	No unresolved High/Critical incidents	Executive and Board reporting.

16.3 Regulatory change monitoring

Compliance and Legal must monitor regulatory developments relevant to crypto, gaming, AML/CFT/CPF, sanctions, Travel Rule, VASP/CASP obligations, stablecoins, data protection, tax and customer protection. Material changes must be assessed for applicability, impact, implementation owner, deadline, procedure changes, training needs and Board/Risk Committee reporting.

17. Training, Awareness, Exceptions and Policy Breaches

Employees and contractors involved in crypto activity must understand the risks and controls relevant to their role. Training must be practical, scenario-based and updated as typologies, regulations and internal processes change.

17.1 Training requirements

Audience	Minimum training content	Frequency
All relevant staff	Crypto basics, irreversibility, customer impact, escalation channels, sanctions awareness, red flags, data handling and incident reporting.	On joining and annually.
Payments / Operations	Deposit and withdrawal workflows, wallet screening, holds, customer communications, unsupported networks, reconciliation handoffs and escalation.	On role assignment and at least annually.
Compliance / MLRO team	Blockchain analytics, typologies, case management, EDD, source of funds, Travel Rule, sanctions, reporting decisions and quality assurance.	At least annually and when major typologies emerge.
Treasury / Finance	Exposure limits, valuation, conversion, stablecoin risk, reconciliations, provider risk, accounting evidence and market disruption playbooks.	At least annually.
Technology / Security / Signers	Wallet architecture, key management, phishing, MFA, PAM, signing procedures, incident response, recovery and secure change management.	At least annually and before signing authority is granted.
Board / Senior Management	Risk appetite, regulatory developments, key incidents, emerging threats, governance duties and strategic decisions.	At least annually or through committee briefings.

17.2 Exceptions

Policy exceptions must be rare, time-bound, risk-assessed and approved at a level commensurate with residual risk. Exceptions involving sanctions, confirmed suspicious activity, licensing breaches, known wallet compromise or prohibited assets are not permitted unless Legal and MLRO determine that a specific legal obligation requires a controlled action. All exceptions must be recorded in the exception register with owner, rationale, compensating controls, expiry date and closure evidence.

17.3 Policy breaches

Any suspected breach of this policy must be reported immediately to the relevant manager and to Risk, Compliance or Information Security as appropriate. Breaches may result in access removal, transaction holds, customer remediation, provider suspension, disciplinary action, contract termination, regulatory reporting, law enforcement referral or other corrective action. The Company prohibits retaliation against employees who report concerns in good faith.

18. Assurance, Testing, Review and Approval

The effectiveness of this policy depends on evidence and testing. Controls must be tested using management self-assessment, Compliance quality assurance, Information Security testing, reconciliation review, vendor assurance and Internal Audit or independent external review. Findings must be risk-rated, assigned to owners and tracked to closure.

18.1 Minimum testing programme

Testing activity	Minimum frequency	Owner
Crypto risk assessment refresh	Annually and upon material trigger	Risk / Compliance
Transaction monitoring rule review	Quarterly and after typology change	Compliance / MLRO
Sanctions screening effectiveness review	Quarterly	Compliance
Wallet access review	Quarterly and upon staff changes	CISO
Key recovery tabletop or technical test	At least annually; after material change	CISO / Treasury
Hot/cold wallet reconciliation review	Daily operational; monthly management review	Finance
Vendor risk review	Annually; high-risk vendors more frequently	Vendor Owner / Risk

Testing activity	Minimum frequency	Owner
Penetration test / security assessment	Annually and after material architecture change	CISO
Incident response tabletop	At least annually	CISO / Risk / Compliance
Independent audit or assurance review	Annually or as directed by the Board/Risk Committee	Internal Audit / External Assurance

18.2 Review triggers

This policy must be reviewed at least annually and sooner if there is a material regulatory change, new licence requirement, new asset or network, new PSP/custodian, material incident, control failure, Board or regulator instruction, significant market event, sanctions typology, internal audit finding, change to business model or expansion into a new jurisdiction.

18.3 Approval

The Risk & Compliance Department owns this policy. The CFO, COO, CCO/MLRO, CISO and Legal must review material revisions. The Board of Directors or delegated Risk Committee approves the policy and any material risk appetite changes. Approval minutes and sign-off evidence must be retained with the policy record.

Approval role	Name / title	Signature	Date
Document Owner	Head of Risk & Compliance		
MLRO / CCO	Chief Compliance Officer / Money Laundering Reporting Officer		
CISO	Chief Information Security Officer		
CFO / COO	Executive Sponsor		
Board / Risk Committee	Chair or delegated authority		

Appendix A - Definitions

Term	Definition
Crypto-asset / digital asset / virtual asset	A digital representation of value that can be digitally transferred, stored or traded, including cryptocurrencies and certain tokens, but excluding digital representations of fiat currency unless treated as a crypto-asset by applicable law.
VASP / CASP	Virtual Asset Service Provider or Crypto-Asset Service Provider, depending on the applicable regulatory framework. This may include exchanges, custodians, transfer services and other crypto service providers.
Travel Rule	Requirement for relevant payment or crypto asset transfer providers to obtain, hold and transmit required originator and beneficiary information in connection with qualifying transfers.
Unhosted wallet / self-hosted wallet	A wallet not held with or controlled by an obliged financial institution, VASP or CASP.
Hot wallet	Wallet connected to online systems and used for operational liquidity or customer withdrawals, carrying elevated cyber risk.
Cold storage	Wallet or custody arrangement kept offline or otherwise isolated from routine online access for stronger protection of retained assets.
MPC / HSM	Multi-party computation or hardware security module technology used to protect signing authority and reduce single-key compromise risk.
Mixer / tumbler	A service, protocol or technique designed to obscure the origin, destination or ownership trail of crypto-assets.
Source of funds	The origin of the specific funds used for a transaction or account activity.
Source of wealth	The origin of the customer's overall wealth or financial standing.
Residual risk	Risk remaining after controls are applied.

Appendix B - Customer and Wallet Risk Scoring Matrix

The following matrix is a minimum standard. Compliance may adopt more granular scoring in case management tooling. A single severe indicator may override the total score and require high-risk or prohibited classification.

Risk factor	Low	Medium	High	Prohibited / exit
Customer identity	Verified, consistent and current.	Minor gaps pending refresh.	EDD required; inconsistencies or high-risk profile.	False identity, forged documents or refusal to provide required information.
Jurisdiction	Allowed, low-risk jurisdiction.	Moderate risk or data inconsistency.	High-risk or weak AML jurisdiction nexus.	Sanctioned or prohibited jurisdiction nexus.
Wallet exposure	Clean history and reputable exchange exposure.	Limited indirect high-risk exposure.	Material high-risk exposure or complex obfuscation.	Direct sanctions, mixer, darknet, ransomware, terrorist financing or stolen funds exposure.
Transaction behaviour	Consistent with profile.	Moderately unusual volume or velocity.	Unexplained high volume, structuring, rapid in/out or chain-hopping.	Confirmed fraud, mule activity or evasion.
Source of funds	Reasonably understood.	Additional evidence desirable.	Evidence required; explanation weak or complex.	Cannot be verified or appears illicit.
Responsible gaming	No indicators.	Mild early warnings.	Repeated risky behaviour or attempts to bypass controls.	Customer harm requiring account restriction under RG policy.

Appendix C - Digital Asset Approval Checklist

Checklist area	Questions to answer	Required evidence
Business rationale	Why is the asset needed? Which customer segment and payment flow will use it? What alternatives exist?	Business case and expected volumes.
Legal/regulatory	Is the asset or service regulated? Are customer disclosures, licence, registration, notification or geographic restrictions needed?	Legal memo and Compliance sign-off.
Financial crime	What typologies affect the asset/network? Is analytics coverage sufficient? Can sanctions and Travel Rule controls operate effectively?	AML risk assessment and monitoring scenarios.
Market/liquidity	Is there sufficient liquidity and price reliability? What volatility and slippage are expected?	Treasury assessment and exposure limits.
Technology/security	Can wallets, confirmations, APIs, keys and monitoring be securely supported?	CISO architecture/security review.
Operations	Are deposits, withdrawals, unsupported networks, customer disclosures and reconciliation procedures ready?	SOPs, testing evidence, training.

Checklist area	Questions to answer	Required evidence
Provider support	Which PSP/custodian/exchange supports the asset and what are their limits and controls?	Vendor due diligence and contracts.
Approval	Who approves launch and what conditions apply?	Risk Committee or delegated approval record.

Appendix D - Crypto Transaction Approval Matrix

The values below are policy defaults and should be calibrated in the Company's authority matrix. Lower thresholds may apply by asset, customer risk tier, jurisdiction or provider.

Transaction / action	Default approval	Required evidence
Customer withdrawal within rules	Automated approval subject to monitoring; Operations oversight.	System screening and transaction log.
Customer withdrawal with alert	Compliance review and Operations manager release.	Case note and decision rationale.
High-risk customer withdrawal	MLRO or delegate approval.	EDD and wallet screening evidence.
Treasury sweep/refill	Treasury plus Security/Operations.	Ticket, whitelisted address, balance limit check.
New treasury/custodian address	CFO, CISO and Compliance.	Out-of-band verification, due diligence, change approval.
Material cold storage movement	3-of-5 multi-signature including Finance, Security and Risk/Compliance.	Full transaction ticket, committee notice and reconciliation.
Exception to policy	CRO/CCO/CISO/CFO as relevant; Risk Committee for high residual risk.	Exception form, compensating controls and expiry date.

Appendix E - Sample Crypto KRIs and Evidence Sources

KRI / KPI	Source evidence	Frequency
Number and value of crypto deposits/withdrawals by asset and jurisdiction	PSP reports, wallet logs, finance ledger	Daily/monthly
High-risk alerts by typology and age	Case management system	Weekly/monthly
Sanctions hits and false-positive rates	Screening tool and case notes	Weekly/monthly
Hot wallet exposure and sweep exceptions	Wallet/custodian reports	Daily
Unreconciled breaks by age and value	Finance reconciliation tool	Daily/monthly
Provider outages and SLA breaches	Vendor dashboard and incident tickets	Monthly
Travel Rule transfer exceptions	Provider/Travel Rule solution reports	Monthly
EDD overdue and source-of-funds requests outstanding	Compliance case management	Weekly/monthly
Training completion by role	Learning management system	Monthly during cycle
Open audit/control findings	Issue tracker	Monthly/quarterly

Appendix F - Incident Severity Matrix

Severity	Financial / asset impact	Regulatory / legal impact	Customer / operational impact
Critical	Material loss, unrecoverable wallet compromise, systemic provider insolvency exposure.	Licence threat, sanctions breach, terrorist financing, major data breach or mandatory immediate reporting.	Widespread customer impact, prolonged withdrawal failure, severe reputational harm.
High	Significant but containable loss or exposure, high-value transfer error, material reconciliation break.	Likely regulator/FIU notification or formal legal assessment required.	Material service disruption, customer complaints, delayed withdrawals.
Medium	Limited financial exposure or controlled operational error.	No immediate reporting expected but control breach requires review.	Limited customer impact or process backlog.
Low	No material loss; issue corrected quickly.	No regulatory impact expected.	No or minimal customer impact.

Appendix G - RACI Summary

Activity	Board / Risk Committee	Risk	Compliance / MLRO	CISO	Finance / Treasury	Operations / Payments	Legal
Approve risk appetite	A	R/C	C	C	C	C	C
Crypto risk assessment	C/A for high risk	R	C	C	C	C	C
Asset approval	A for material	R/C	C	C	C	R/C	C
CDD/EDD and SAR/UTR decisions	I	C	A/R	C as needed	I	R for inputs	C
Wallet/key security	I	C	C	A/R	C	R for operations	C
Treasury exposure	I/A for limits	C	C	C	A/R	I	C
Vendor due diligence	I/A for high risk	R	C	C	C	R for owner	C
Incident response	I/A for critical	C	C/R	A/R	C/R	R	C/R
Policy review	A	R	C	C	C	C	C

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed.

Appendix H - Regulatory and Standards Reference Sources

This appendix identifies public sources considered in drafting this policy. The Company must monitor updates to these sources and any local legal advice, regulator instructions or licence conditions that apply to its activities.

Source	Relevance to this policy
Financial Action Task Force (FATF) - Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs (2021)	Risk-based approach, CDD, counterparty VASP due diligence, Travel Rule, unhosted wallet considerations, AML/CFT controls and sanctions screening.
FATF - Virtual Assets: Targeted Update on Implementation of FATF Standards on VAs and VASPs (2025)	Current implementation gaps, global Travel Rule progress and need for stronger supervision, risk assessment and mitigation.
Curaçao Gaming Authority - LOK / Online Gaming Portal / AML-CFT-CPF publications and notifications	Gaming licence context, AML/CFT supervision, periodic/incident/change reporting, FATF/CFATF and sanctions notices for the Curaçao gaming industry.
European Securities and Markets Authority (ESMA) - Markets in Crypto-Assets Regulation (MiCA)	EU crypto-asset market rules, authorisation and supervision considerations for crypto-asset services where EU scope applies.
European Banking Authority (EBA) - Travel Rule Guidelines under Regulation (EU) 2023/1113	Information requirements and procedures for missing or incomplete information in transfers of funds and crypto-assets where EU scope applies.
NIST Cybersecurity Framework 2.0	Cybersecurity governance, identify, protect, detect, respond and recover control outcomes for wallet and technology risk management.
ISO 31000:2018 Risk Management - Guidelines	Enterprise risk management principles, risk assessment, treatment, monitoring and continuous improvement concepts.

End of Policy