

Jer-Team N.V.

Risk Policy for Crypto Usage

1. Purpose

This Risk Policy establishes Jer-Team N.V.'s framework for the responsible, secure, and compliant use of crypto-assets in the context of its licensed online gaming operations.

The objectives of this Policy are as follows:

1.1. Regulatory Alignment:

- Ensure compliance with the Curaçao Gaming Control Board (CGA) requirements, particularly regarding Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Responsible Gaming obligations.
- Align with the Financial Action Task Force (FATF) recommendations on Virtual Asset Service Providers (VASPs), including customer due diligence, transaction monitoring, and reporting of suspicious activities.
- Take into consideration applicable EU/EEA regulatory frameworks, such as the Markets in Crypto-Assets Regulation (MiCA), the 5th and 6th EU Anti-Money Laundering Directives, and GDPR obligations.

1.2. Risk Identification and Mitigation:

- Identify inherent risks linked to the acceptance and processing of crypto-assets, including money laundering, terrorist financing, fraud, market volatility, cybersecurity breaches, and regulatory uncertainty.
- Establish robust internal controls to mitigate these risks without disrupting legitimate player activity or compromising the entertainment value of gaming operations.

1.3. Operational Integrity:

- Define clear standards for how crypto-assets are integrated into payment flows (deposits, wagering, withdrawals) in a secure, auditable, and transparent manner.
- Maintain the integrity of financial operations by ensuring segregation of funds, secure custody of company wallets, and reliable transaction records.

1.4. Player Protection and Transparency:

- Safeguard players by implementing mechanisms to protect against irresponsible gambling behavior related to crypto's perceived anonymity and volatility.
- Provide transparent disclosures to players about the unique characteristics of crypto-assets, including irreversibility of transactions and potential fluctuations in value.

1.5. Corporate Governance:

- Clarify the responsibilities of the Board of Directors, Compliance Officers, and operational staff in managing crypto-related risks.
- Support a culture of compliance and accountability, where crypto-related decisions are subject to appropriate oversight, internal audit, and external regulatory review.

In summary, this Policy ensures that Jer-Team N.V.'s use of crypto-assets is responsible, transparent, secure, and compliant with all relevant legal and regulatory frameworks, while fostering innovation and maintaining the trust of regulators, players, and business partners.

2. Scope

This Policy applies to all activities within Jer-Team N.V. where crypto-assets are accepted, processed, or otherwise integrated into the company's online gaming ecosystem. Specifically, it covers:

2.1. Players and End-Users:

- All individuals using cryptocurrencies for deposits, wagers, in-game transactions, and withdrawals.
- Both newly registered and existing players, regardless of their jurisdiction, who interact with Jer-Team N.V.'s platforms via crypto-assets.
- Situations where players combine fiat and crypto transactions, requiring hybrid monitoring and reporting.

2.2. Employees and Internal Staff:

- All employees directly handling crypto-related operations, including Compliance, Finance, Risk Management, IT, and Customer Support teams.
- Senior management and the Board of Directors, who retain ultimate responsibility for crypto-risk oversight and governance.
- Any internal staff with access to systems that process, store, or report crypto transactions.

2.3. Contractors and Third-Party Service Providers:

- Payment processors, wallet providers, blockchain analytics partners, and custodians engaged by Jer-Team N.V..
- Technology vendors providing transaction monitoring, anti-fraud, and AML screening solutions.
- Any consultants, auditors, or outsourced compliance teams involved in crypto-related operations.

2.4. Business Units and Functional Areas:

- Finance & Treasury: responsible for wallet management, liquidity control, and safeguarding of company reserves.
- Operations: managing integration of crypto payment gateways and ensuring smooth transaction flows.

- Compliance & Risk: enforcing AML/CTF controls, sanctions screening, and transaction monitoring.
- IT & Security: responsible for safeguarding wallet infrastructure, access controls, and cybersecurity protocols.
- Customer Support: ensuring transparent communication with players on crypto usage, risks, and transaction handling.

2.5. Operational Flows Covered:

- Acceptance of crypto-assets as a method of payment (deposits and wagers).
- Payouts and withdrawals to player wallets.
- Conversion between crypto and fiat where applicable.
- Custody, storage, and security of operational and reserve crypto wallets.
- Record-keeping, monitoring, and reporting of all crypto transactions in compliance with Curaçao CGA and FATF standards.

3. Key Risks Identified

Jer-Team N.V. acknowledges that the integration of crypto-assets into online gaming operations introduces specific risks that must be proactively managed. The following categories of risks have been identified:

3.1. Money Laundering and Terrorist Financing (ML/TF):

- Use of cryptocurrencies to conceal the source of illicit funds, including placement, layering, and integration schemes.
- Attempted circumvention of traditional banking due diligence by exploiting pseudonymous or unhosted wallets.
- Transactions linked to sanctioned entities, high-risk jurisdictions, politically exposed persons (PEPs), or darknet marketplaces.

3.2. Fraud and Scams:

- Fraudulent deposits or manipulation of transaction timestamps and confirmations to exploit system delays.
- Crypto-fiat conversion fraud through unregulated exchanges or unverified payment intermediaries.
- “Chargeback-style” disputes where players attempt to reverse crypto payments via external services or claim non-receipt of withdrawals.

3.3. Market Volatility:

- High volatility of cryptocurrencies that can result in significant fluctuations between the time of deposit and withdrawal, affecting both operator and player balances.
- Liquidity risk arising from sudden changes in exchange rates or reduced market access during periods of instability.
- Reputational risk if volatility leads to disputes or perceived unfair treatment of players.

3.4. Technology and Cybersecurity Risk:

- Vulnerabilities in wallet infrastructure (hot vs. cold storage), including risk of hacking, phishing, or malware attacks.
- Private key compromise leading to theft or permanent loss of assets.
- Dependence on third-party exchanges, custodians, and payment processors, which may be subject to operational failures or cyberattacks.

3.5. Regulatory and Legal Uncertainty:

- Rapidly evolving legal requirements across jurisdictions where players are based, leading to inconsistent obligations.
- Uncertainty regarding tax treatment, licensing conditions, and classification of crypto-assets under Curaçao and international frameworks.
- Potential enforcement actions or penalties in case of non-compliance with AML/CTF obligations or misalignment with FATF guidance.

3.6. Player Protection and Responsible Gaming Risks:

- Increased risk of excessive or impulsive gambling due to perceived anonymity and ease of transferring funds.
- Potential misuse of crypto-assets to mask gambling activity from financial institutions or family members.
- Lack of awareness among players of the risks associated with volatility, irreversibility of transactions, and security of personal wallets.

3.7. Operational and Reputational Risks:

- Failure to implement adequate crypto risk management may result in fines, license suspension, or reputational damage.
- Association with illicit crypto activities (even unintentionally) can harm the company's brand and regulator trust.

4. Risk Mitigation Measures

Jer-Team N.V. has established a multi-layered risk control framework to ensure that all crypto-related risks are effectively identified, managed, and mitigated. The following measures are applied across the organization:

4.1. AML/CTF Controls

- **Enhanced KYC:** All players engaging in crypto transactions must undergo enhanced customer due diligence (eCDD), including proof of identity, proof of address, and source of funds verification where applicable.
- **Blockchain Analytics:** Use of blockchain monitoring tools (e.g., Chainalysis, Elliptic, TRM Labs) to trace wallet activity, identify potential connections to illicit activity, and assess transaction risk scores.

- **Sanctions Screening:** All wallet addresses and counterparties are screened against UNSC, EU, OFAC, and local Curaçao sanctions lists. Any hits result in immediate escalation to the Compliance Officer.
- **Suspicious Activity Reporting:** All unusual or suspicious crypto transactions are reported without delay to the Financial Intelligence Unit (FIU) Curaçao, in line with the National Ordinance on the Reporting of Unusual Transactions (NORUT).
- **Prohibited Assets:** Privacy-enhancing coins (e.g., Monero, Zcash, Dash PrivateSend) or tokens with insufficient traceability are not accepted under any circumstances.

4.2 Transaction Monitoring

- **Real-Time Monitoring:** A dedicated monitoring system tracks all crypto deposits and withdrawals in real time.
- **Red-Flag Indicators:** Alerts are triggered for transactions involving:
 - High-value deposits inconsistent with the player's profile or activity history.
 - Rapid withdrawals shortly after deposits (potential layering).
 - Multiple wallet addresses linked to the same user account.
 - Connections to mixers, tumblers, or high-risk exchanges.
- **Threshold Controls:** Automated alerts for transactions exceeding pre-defined limits (both fiat-equivalent thresholds and cumulative daily/weekly amounts).
- **Escalation Protocol:** Transactions flagged by the monitoring system are immediately reviewed by the AML/Compliance team, with authority to freeze or block suspicious activity.

4.3 Custody and Wallet Security

- **Wallet Segregation:**
 - *Cold storage wallets* are used for company reserves, requiring multi-signature authorization for any transaction.
 - *Hot wallets* are maintained for operational liquidity only, with strict daily exposure caps.
- **Access Controls:** Wallets are secured with multi-factor authentication, restricted access rights, and periodic key rotation.
- **Penetration Testing:** Regular penetration tests and security audits are conducted to identify and remediate vulnerabilities.
- **Disaster Recovery:** Secure backup procedures for private keys and recovery protocols in case of system compromise.

4.4 Player Protection

- **Risk Disclosures:** Players are provided with clear disclosures on the risks of volatility, irreversibility, and transaction processing times for crypto-assets.
- **Deposit & Loss Limits:** Crypto deposits are subject to mandatory player protection limits (per transaction, daily, and monthly).
- **Behavioral Monitoring:** Responsible gaming tools monitor abnormal betting patterns (e.g., rapid large deposits, repeated losses funded by crypto wallets).
- **Cooling-Off Measures:** Players showing signs of risky behavior may be subject to temporary restrictions or prompted to set lower deposit limits.

4.5 Regulatory Compliance

- **Ongoing Monitoring:** Jer-Team N.V. maintains continuous review of Curaçao CGA guidelines, FATF recommendations, and developments under EU AML directives and MiCA.
- **Staff Training:** Compliance, operations, and finance staff receive regular training on crypto-specific risks, suspicious transaction reporting, and emerging typologies.
- **Third-Party Oversight:** Jer-Team N.V. only partners with licensed, reputable crypto payment processors and custodians. All vendors are subject to due diligence and contractual compliance obligations.
- **Audit and Reporting:** Regular internal audits and external reviews ensure adherence to this Policy. Results are documented and made available to regulators upon request.

5. Governance

Jer-Team N.V. maintains a clear governance structure to ensure that crypto-related risks are subject to robust oversight, accountability, and transparent reporting. The following roles and responsibilities apply:

5.1. Board of Directors

- Holds ultimate accountability for crypto risk management within Jer-Team N.V..
- Approves this Policy and any amendments thereto.
- Reviews quarterly compliance reports prepared by the Compliance Officer, including details of crypto transaction monitoring, suspicious activity reports (SARs), and operational incidents.
- Ensures sufficient resources (staff, tools, training, and budget) are allocated for effective crypto risk management.
- Provides strategic direction in line with Curaçao Gaming Control Board (CGA) regulatory requirements and FATF standards.

5.2. Compliance Officer

- Responsible for day-to-day implementation and enforcement of this Policy.
- Conducts ongoing monitoring of crypto transactions, customer onboarding, and AML/CTF obligations.
- Escalates suspicious or high-risk activity to the FIU Curaçao and, when appropriate, to the Board.
- Maintains an internal register of crypto-related risks, incidents, and remediation measures.
- Provides quarterly compliance reports to the Board and ad-hoc updates in case of material risk events.

5.3. Finance & Operations Teams

- Manage liquidity, wallet operations, and reconciliation of crypto transactions.
- Implement segregation of funds between operational hot wallets and reserve cold storage.
- Ensure timely reporting of any anomalies or breaches to the Compliance Officer.

5.4. IT & Security Teams

- Maintain the security and resilience of wallet infrastructure, private keys, and transaction systems.
- Conduct regular penetration testing, vulnerability assessments, and implement remediation plans.
- Report cybersecurity incidents immediately to the Compliance Officer and Board.

5.5. Internal Audit Function

- Performs independent reviews of crypto risk controls at least once annually.
- Verifies compliance with Curaçao AML/CTF requirements, FATF recommendations, and internal policies.
- Provides audit findings directly to the Board of Directors, ensuring independence from operational management.

5.6. External Oversight

- Jer-Team N.V. engages qualified external auditors and consultants when required to validate its crypto controls.
- Audit outcomes and regulator feedback are documented and addressed through corrective action plans approved by the Board.

6. Review and Updates

Jer-Team N.V. recognizes that crypto-related risks and regulatory requirements evolve rapidly. To ensure ongoing relevance and effectiveness, this Policy is subject to a structured review and update process as follows:

6.1. Review Frequency

- This Policy shall be formally reviewed at least once per year by the Compliance Officer in coordination with the Finance, IT, and Operations teams.
- An extraordinary review will be initiated earlier than annually if triggered by:
 - Regulatory changes (e.g., new CGA directives, FATF recommendations, EU AML/MiCA updates).
 - Technological changes (e.g., new wallet infrastructure, payment gateways, blockchain protocols).
 - Operational incidents (e.g., security breach, suspicious transaction trends, audit findings).
 - External developments (e.g., sanctions updates, emergence of new high-risk crypto typologies).

6.2. Amendment Process

- Proposed changes are drafted by the Compliance Officer, in consultation with relevant departments.
- Amendments undergo internal review by Legal, Finance, and IT teams to ensure accuracy and operational feasibility.

- Final approval of amendments rests with the Board of Directors, which holds ultimate responsibility for crypto risk governance.

6.3. Documentation and Record-Keeping

- All reviews, amendments, and approvals must be documented in the Policy Review Log maintained by the Compliance Officer.
- Historical versions of this Policy are archived and retained for a minimum of five years, in line with Curaçao compliance requirements.

6.4. Regulatory Communication

- Any material changes to this Policy, if requested, shall be communicated to the Curaçao Gaming Control Board (CGA) and/or other competent authorities.
- Jer-Team N.V. commits to full cooperation with regulators in providing updated documentation upon demand.

6.5. Awareness and Training

- Following each update, all relevant employees and contractors will be notified of the changes and provided with appropriate training where necessary.
- Updated versions of this Policy shall be circulated internally and made available for inspection by auditors and regulators.