

CRYPTOCURRENCY RISK MANAGEMENT POLICY

Genco Pura B.V. operates as a global online gambling and entertainment platform that supports cryptocurrency-based deposits, wagers, and withdrawals. As a platform that processes high-volume, real-time digital asset transactions, Genco Pura B.V. adopts a comprehensive risk management framework designed to safeguard users, protect platform integrity, and ensure compliance with applicable regulatory and industry standards.

Introduction

Genco Pura B.V. recognizes that cryptocurrency presents unique operational, financial, compliance, and cybersecurity risks arising from its decentralized structure, global accessibility, and rapid technological evolution. Unlike traditional financial systems, digital assets operate on public blockchains where transactions are pseudonymous, irreversible, and often outside the control of central authorities. These characteristics increase exposure to threats such as wallet compromise, fraud, cyberattacks, market volatility, regulatory uncertainty, and operational disruptions caused by blockchain congestion or smart-contract failures. Given the scale and real-time nature of Genco Pura B.V.'s platform activity, the Company must adopt a comprehensive and proactive approach to safeguarding the integrity of crypto transactions and user funds. Effective risk management requires coordinated efforts across governance, technology, compliance, operations, and security teams, with clearly defined processes for oversight, escalation, and continuous improvement.

This Policy therefore establishes the principles, standards, and controls governing the identification, assessment, mitigation, and monitoring of crypto-related risks across Genco Pura B.V.'s operations. It sets a unified framework for managing blockchain-based value flows, ensures compliance with applicable laws and industry expectations, and articulates the Company's commitment to maintaining a secure, transparent, and resilient crypto-enabled environment for all users.

Governance and Responsibility

The management of cryptocurrency risk at Genco Pura B.V. is overseen by the Risk & Compliance Team, which includes senior representatives from Legal & Compliance, IT Security, Finance, Fraud Prevention, and Customer Support. This multidisciplinary structure ensures that decisions related to crypto risk are informed by operational realities, regulatory developments, technological evolution, and user behavior patterns. Genco Pura B.V.'s governance framework emphasizes accountability, transparency, and continuous oversight. The Risk & Compliance Team is responsible for establishing crypto-specific risk thresholds, reviewing incidents, approving key control changes, and coordinating with external stakeholders such as regulators, custodians, auditors, and blockchain analytics partners. The Team also ensures that Genco Pura B.V.'s policies and procedures remain aligned with industry best practices and applicable laws across all jurisdictions in which the Company operates.

Our governance structure also includes periodic oversight by Senior Management, which reviews crypto-related performance metrics, incident trends, liquidity reports, and compliance risks. Major strategic changes, such as onboarding new custodians or adopting new blockchain technologies, require approval from Senior Management to ensure ongoing operational resilience and regulatory compliance.

Genco Pura B.V.

163609

Abraham Mendez Chumaceiro Blvd. 03, Willemstad, Curaçao

Risk Identification

Genco Pura B.V. identifies cryptocurrency risks across multiple interconnected domains, reflecting the complexity and decentralized nature of digital asset ecosystems. By adopting a structured approach to risk identification, the Company ensures that both emerging and established threats are continuously recognized, understood, and assessed.

Key categories of crypto-related risks include:

Market Volatility Risk: Cryptocurrency prices can fluctuate dramatically within short periods, potentially affecting the value of assets held in hot or cold wallets before conversion or settlement. Genco Pura B.V. monitors market conditions and maintains liquidity strategies to manage exposure to rapid price movements.

Operational Risk: Crypto-related workflows—such as deposit processing, withdrawal handling, wallet maintenance, and reconciliation—introduce operational vulnerabilities. Errors, delayed blockchain confirmations, system outages, inadequate segregation of duties, or manual mistakes can disrupt service delivery and create financial or reputational exposure.

Cybersecurity and Private Key Risk: The irreversible nature of blockchain transactions amplifies the impact of unauthorized access or compromised private keys. Genco Pura B.V. identifies risks stemming from malware, phishing, SIM swaps, infrastructure attacks, smart contract exploits, and internal security lapses. These risks highlight the need for hardened infrastructure, strong authentication, and secure key management.

Blockchain Network Risk: Network congestion, protocol upgrades, chain reorganizations, or network attacks (e.g., 51% attacks) can affect the speed, reliability, and predictability of blockchain transactions. Genco Pura B.V. continuously monitors network health indicators to mitigate the risk of delayed or failed transactions.

Regulatory and Compliance Risk: The global regulatory landscape for cryptocurrency is rapidly evolving. Genco Pura B.V. identifies risks tied to changes in licensing requirements, reporting obligations, sanctions rules, AML/CFT expectations, and cross-border restrictions. These risks are heightened in jurisdictions where digital asset frameworks are unclear or newly emerging.

Fraud and User-Driven Risk: Cryptocurrency's pseudonymous nature enables fraud schemes such as account takeovers, identity fraud, bonus abuse, chargeback-style scams (in fiat on/off-ramps), and collusion. Genco Pura B.V. employs behavioral analytics and blockchain monitoring tools to detect suspicious user activity and prevent financial crime.

Third-Party and Smart Contract Risk: Genco Pura B.V. relies on external service providers—including custodians, exchanges, liquidity partners, and blockchain analytics vendors. Each provider introduces operational and security risks. For platforms integrating smart contracts or decentralized protocols, additional risk arises from bugs, vulnerabilities, or manipulation.

Each identified risk is formally documented within Genco Pura B.V.'s enterprise risk register. Risks are reviewed periodically or whenever new blockchain technologies, regulatory changes, or platform

features emerge. This ensures that crypto-related risks remain aligned with strategic objectives, operational priorities, and regulatory expectations.

Risk Assessment

Once risks have been identified, Genco Pura B.V. conducts a structured and repeatable assessment process to determine their severity, potential impact, and the degree of control required. Risk assessment incorporates both quantitative and qualitative factors to ensure a holistic understanding of each threat and its implications for the platform.

Genco Pura B.V. evaluates risks based on the following key dimensions:

Likelihood of Occurrence: The probability that a particular risk event such as a cyberattack, wallet compromise, custodian outage, or blockchain congestion will materialize. Likelihood is assessed using historical data, threat intelligence, behavioral analytics, and industry trends.

Financial Impact: The potential monetary loss associated with a risk event. This may include direct loss of digital assets, operational downtime, liquidity disruption, regulatory fines, or increased operational costs. Financial impact models help Genco Pura B.V. understand worst-case, expected, and probable loss scenarios.

Customer Harm: The potential effect on users, including delayed withdrawals, loss of access, compromised accounts, or financial loss due to fraudulent activity. Risks that may materially affect customer trust or safety receive elevated prioritization.

Reputational Effect: Crypto-related incidents can significantly damage platform credibility. Genco Pura B.V. assesses reputational consequences by considering how each risk may affect user confidence, media perception, investor trust, and regulatory scrutiny.

Regulatory and Legal Implications: Crypto risk events may trigger reporting obligations, license reviews, investigations, or enforcement actions. Genco Pura B.V. evaluates each risk in light of the regulatory expectations of the jurisdictions in which it operates.

Risk assessments are updated routinely or on an ad hoc basis when new threats, technologies, or platform features emerge. This dynamic approach ensures that the Company's control environment evolves with changing market conditions, regulatory updates, and advancements in cyber and blockchain technology.

Operational Controls and Wallet Management

Genco Pura B.V. recognizes that cybersecurity is a foundational pillar of its cryptocurrency operations due to the irreversible, high-value, and globally accessible nature of digital asset transactions. To safeguard user funds, platform integrity, and internal systems, Genco Pura B.V. employs a multi-layered cybersecurity architecture designed to prevent, detect, and respond to advanced threats targeting both blockchain-related and traditional IT infrastructure.

Genco Pura B.V. operates under a strict zero-trust security model, which assumes no user, device, or network segment is inherently trustworthy. Access to sensitive environments is granted strictly on the

basis of least privilege, with continuous authentication, granular permission controls, and real-time session monitoring. This ensures that only authorized and verified personnel may interact with critical systems such as wallet infrastructure, internal consoles, and administrative tools.

To fortify network resilience, Genco Pura B.V. deploys enterprise-grade firewalls, load balancers, intrusion detection and prevention systems (IDPS), and DDoS mitigation technologies. These systems filter malicious traffic, prevent unauthorized access attempts, and ensure that the platform remains stable during high-volume attacks. Network segmentation further reduces risk by isolating wallet systems, key-management hardware, and back-office tools from public-facing services.

On the device level, Genco Pura B.V. enforces endpoint detection and response (EDR) protections that continuously scan for malware, suspicious behavior, or unauthorized configuration changes. All employee devices connected to sensitive systems are encrypted, monitored, and secured with multi-factor authentication and strict patch-management policies.

Genco Pura B.V. maintains strict private-key security controls, including the use of hardware security modules (HSMs), multisignature authorization workflows, encrypted key backups, and geographically distributed secure environments. Each key operation requires multiple approvers, ensuring no single individual has unilateral control over digital assets.

Where smart contracts or external blockchain applications are used, Genco Pura B.V. subjects them to independent code audits, penetration testing, and continuous monitoring to detect vulnerabilities or unexpected behavior. Application-layer protection such as Web Application Firewalls (WAF), rate limiting, and encrypted API communication add additional defensive layers.

Genco Pura B.V.'s 24/7 security operations center (SOC) monitors platform activity using real-time analytics, machine-learning threat detection, log aggregation, and anomaly identification tools. Alerts are escalated to incident response teams for rapid containment and investigation.

In the event of a cyber incident, Genco Pura B.V. activates a detailed incident response and crisis-management plan, covering immediate isolation, forensic analysis, evidence preservation, user communication, and regulatory notification where required. Regular tabletop exercises and simulated attacks ensure continuous preparedness.

Finally, all third-party integrations—including custodians, exchanges, analytics providers, and cloud service suppliers—undergo rigorous security due diligence, API monitoring, SLA review, and ongoing risk assessments. Genco Pura B.V. ensures that external partners meet or exceed its internal security standards before handling any blockchain-related processes.

Cybersecurity and Infrastructure Security

Genco Pura B.V. maintains a robust cybersecurity and infrastructure security framework designed to protect the platform, its users, and digital assets from evolving threats in the cryptocurrency and online-gaming environment. Because disruptions or breaches can lead to irreversible asset loss and significant reputational harm, Genco Pura B.V. employs a multi-layered strategy that combines advanced technology, strict governance, and continuous monitoring.

At the core of its defenses, Genco Pura B.V. employs end-to-end encryption to secure data in transit and at rest, ensuring that sensitive information—including user credentials, wallet data, and internal communication—cannot be intercepted or manipulated. Complementing encryption, intrusion detection and intrusion prevention systems (IDS/IPS) continuously scan network activity for unusual patterns, known attack signatures, or unauthorized access attempts, enabling early detection and immediate response to potential threats.

To mitigate the risk of large-scale disruption, Genco Pura B.V. implements enterprise-grade DDoS mitigation systems capable of identifying and filtering malicious traffic before it reaches the platform. These defenses enable Genco Pura B.V. to maintain operational stability even during coordinated attacks designed to overload servers or disrupt user activity.

Where Genco Pura B.V. interacts with blockchain networks or smart-contract components, the Company subjects these mechanisms to smart contract security reviews, vulnerability scans, and third-party audits. This helps identify coding flaws, logic errors, or exploitable vulnerabilities before they can impact users.

Genco Pura B.V. also conducts continuous penetration testing, both internally and through accredited external cybersecurity firms. These simulated attacks test the strength of defenses across wallet systems, application layers, APIs, administrative tools, and network infrastructure. Findings from these assessments are formally reviewed, documented, and integrated into system hardening efforts.

To ensure relentless vigilance, Genco Pura B.V. operates a 24/7 Security Operations Center (SOC) that monitors platform activity in real time. The SOC uses behavior analytics, threat-intelligence feeds, machine-learning models, and automated alerting tools to identify anomalies such as account compromise attempts, unauthorized wallet movements, sudden traffic spikes, and infrastructure abnormalities. The SOC coordinates with incident response teams to contain and remediate threats immediately.

Redundancy is built into all major infrastructure components, including servers, wallet systems, database clusters, and load balancers. This redundancy ensures that the platform can continue to operate efficiently even if one or more components fail or are taken offline due to planned maintenance or hostile activity. Traffic distribution, mirrored environments, and failover capabilities further reduce the risk of downtime.

Together, these cybersecurity and infrastructure measures provide Genco Pura B.V. with a resilient, secure, and continuous operating environment, capable of withstanding modern cyber threats while delivering reliable service to users around the world.

Compliance, AML/CFT, and Regulatory Oversight

Genco Pura B.V. operates under a rigorous compliance framework designed to uphold global Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) standards. Because cryptocurrency ecosystems can be exploited for anonymity-enhanced transactions and cross-border illicit flows, Genco Pura B.V. implements a comprehensive suite of controls designed to detect, prevent, and report suspicious activity while ensuring full adherence to applicable legal and regulatory requirements.

Genco Pura B.V.'s AML/CFT program begins with a strong Know Your Customer (KYC) foundation. All users must undergo identity verification through government-issued documents, biometric or liveness validation where applicable, and proof-of-ownership checks for deposit and withdrawal channels. Wallets, payment instruments, and external accounts used on the platform must be verified and tied directly to the user to prevent account misuse, impersonation, and third-party laundering.

Every cryptocurrency transaction processed on the platform—whether a deposit, withdrawal, internal transfer, or wallet update—is subjected to automated blockchain analytics screening. This includes checks for exposure to prohibited or high-risk activities such as mixing/tumbling services, darknet markets, ransomware addresses, sanctioned blockchain entities, stolen funds, phishing clusters, or wallets associated with fraud rings. Transactions that trigger risk indicators are automatically flagged, escalated to compliance specialists, or temporarily paused pending enhanced review.

Parallel to blockchain analytics, Genco Pura B.V. employs behavioral and transactional monitoring systems that analyze user activity patterns. These systems detect anomalies such as rapid-fire deposits and withdrawals, inconsistent spending behaviors, multi-accounting, sudden changes in device fingerprints, or access attempts from high-risk jurisdictions. High-risk or suspicious behavior is escalated for manual investigation and, if necessary, subjected to enhanced due diligence (EDD).

Genco Pura B.V. maintains clear AML/CFT governance policies, including risk assessments, transaction-monitoring rules, reporting procedures, sanctions-screening standards, and documentation requirements. The platform conducts periodic AML/CFT training for staff, particularly those in Compliance, Fraud Prevention, Customer Service, and Payments Operations, ensuring personnel remain proficient in evolving typologies and regulatory obligations.

As part of its regulatory obligations, Genco Pura B.V. maintains transparent and cooperative relationships with regulators, financial institutions, auditors, and law-enforcement agencies in the jurisdictions it serves. Where required by law, Genco Pura B.V. files Suspicious Activity Reports (SARs), responds to government requests, and provides relevant transactional records. The Company also participates in regulatory reviews, independent assessments, and supervisory examinations.

To ensure global alignment, Genco Pura B.V. continuously monitors changes in regulatory frameworks—including licensing conditions, crypto-specific rules, gambling regulations, sanctions updates, and cross-border compliance developments. Best-practice standards from FATF, the EU, FinCEN, and other global bodies are incorporated into Genco Pura B.V.'s risk-based AML/CFT program, ensuring the Company remains compliant even across rapidly evolving regulatory environments.

Through this comprehensive compliance, AML/CFT, and oversight structure, Genco Pura B.V. maintains the integrity of its platform, protects users, and contributes to the overall safety and legitimacy of the wider cryptocurrency ecosystem.

Fraud Prevention and User Protection

Genco Pura B.V. employs a multi-layered approach to safeguard users and prevent fraud. Advanced monitoring systems detect unusual activity such as rapid deposits and withdrawals, multi-account attempts, bonus abuse, and suspicious wallet transactions. High-risk activity is flagged for enhanced

review, while machine learning-driven analytics continuously assess user behavior to identify potential threats. Genco Pura B.V. user-centric security measures, including mandatory two-factor authentication (2FA), device fingerprinting, and cooldown periods, help protect accounts and ensure transaction integrity. All fraud prevention measures comply with global AML/CFT standards, with cooperation from regulatory authorities and law enforcement where necessary. These systems are continuously updated to address emerging threats, providing both proactive protection and user confidence in the platform.

Business Continuity and Incident Response

Genco Pura B.V. operates a comprehensive business continuity and incident response framework, specifically designed to address the unique risks associated with cryptocurrency operations. The framework ensures the protection of customer funds, operational resilience, and rapid response to any incidents affecting platform infrastructure or underlying blockchain networks.

The company maintains procedures to respond effectively to a wide range of crypto-related incidents, including wallet compromises, blockchain disruptions, network forks, protocol changes, and attacks targeting infrastructure or smart contracts. Immediate containment and mitigation protocols are in place for unauthorized access or compromised private keys. Blockchain health is continuously monitored to address forks, consensus changes, network congestion, or other disruptions. Genco Pura B.V. is also prepared for updates or changes in blockchain protocols that may affect smart contracts, wallets, or transaction processing. Continuous detection of potential attack vectors targeting system infrastructure, APIs, and smart contracts ensures rapid mitigation and secure recovery.

Customer assets remain secure, auditable, and accessible even during network instability or operational disruption. Critical systems and wallets are designed with redundancy and failover capabilities to ensure uninterrupted service, while key functions, including transaction processing, compliance monitoring, and customer support, are maintained under all circumstances. Following any incident, structured reviews assess root causes, response effectiveness, and lessons learned. Findings are used to enhance policies, technical controls, operational procedures, and staff training, ensuring that the incident response and continuity framework evolves in line with emerging threats.

Clear communication protocols are maintained with customers, partners, and regulatory authorities as required, with timely guidance and alerts provided to affected users to ensure awareness and continued fund protection. Regular simulations, stress tests, and internal audits validate the effectiveness of incident response and business continuity plans. Continuous monitoring of threat intelligence, blockchain vulnerabilities, and industry best practices supports proactive mitigation and preparedness.

Custodial and Third-Party Risk

When Genco Pura B.V. uses external custodians or liquidity partners, it performs due diligence on their security standards, financial stability, regulatory posture, and operational resilience. Genco Pura B.V. remains responsible for safeguarding customer assets and ensures that third-party relationships are governed by strict SLAs, security requirements, and ongoing monitoring.

Market and Liquidity Risk Management

Genco Pura B.V. manages crypto liquidity to ensure uninterrupted user withdrawals and seamless platform operation. Real-time liquidity dashboards, reserve buffers, and multi-currency hedging strategies reduce exposure to volatile price swings. Stablecoin use is managed with due care and subject to thorough risk-rating criteria.

User Education and Transparency

Genco Pura B.V. provides guidance to users on safe crypto practices, including wallet security, phishing awareness, and transaction irreversibility. Platform disclosures help users understand the risks involved in transacting with cryptocurrencies and the steps Genco Pura B.V. takes to mitigate those risks.

Review and Continuous Improvement

The Risk & Compliance Team reviews this Policy annually or sooner when new threats, regulatory changes, or technological shifts arise. Genco Pura B.V. is committed to continuous adaptation and strengthening of its crypto risk posture to remain a trusted leader in crypto-enabled gaming.