

CASTIANES B.V. POLICY
FOR CRYPTO USAGE

VERSION CONTROL

Version	Version Date	Approved By
1.0	07/02/2025	The Board

CONTENTS

VERSION CONTROL..... 1

CONTENTS.....2

ABBREVIATIONS.....3

1. PREAMBLE.....4

THE POLICY.....4

THE PURPOSEError! Bookmark not defined.

2. SCOPE.....Error! Bookmark not defined.

RISK IDENTIFICATION AND ASSESSMENTError! Bookmark not defined.

MITIGATION STRATEGIES.....6

CUSTOMER COMMUNICATION.....7

3. CONCLUSION.....8

4. RATIFICATION9

ABBREVIATIONS

AML.....	Anti Money Laundering
CTF.....	Counter Terrorist Financing
CFP.....	Counter Financing of Proliferation
Curaçao GCB.....	Curaçao Gaming Control Board
FIU.....	Financial Intelligence Unit
MFA.....	Multi-Factor Authentication
ML.....	Money Laundering
MLRO.....	Money Laundering Reporting Officer
SAR.....	Suspicious Activity Report
TF.....	Terrorist Financing

1. PREAMBLE

THE PURPOSE

The Policy outlines the general unified standards and procedures of Risks evolving from operation with cryptocurrencies, which must be adhered to by Castianes B.V. (Hereinafter — «the Company») its directors, officers and employees. Setting up these standards and procedures will ensure legal, financial, and economic stability of the company, as well as for the customers.

Due to the decentralized and pseudonymous nature of cryptocurrencies, they can be susceptible to misuse in illicit activities, including ML, TF, and other financial crimes. It is therefore the responsibility of operators to establish and rigorously follow Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) policies, making it significantly more challenging for criminals to exploit the operator's infrastructure for illegal purposes.

A company that adheres to strict compliance standards for cryptocurrency usage not only minimizes its operational risks but also creates a secure environment for customers. This transparency encourages greater client confidence and may incentivize more customers to adopt cryptocurrency for payments on the company's platform. Furthermore, cryptocurrency offers the advantage of global applicability with reduced transaction costs and faster processing times compared to traditional currency transfers.

For companies in the gambling industry, a robust cryptocurrency policy is critical to navigating the unique legal, financial, and operational complexities associated with digital assets. Such a policy must balance compliance requirements, customer protection, and industry-specific risks. While cryptocurrencies present significant benefits, these associated risks must be managed with a comprehensive policy and risk management framework.

Effective controls and procedures in the cryptocurrency sector serve a dual purpose: safeguarding consumers and protecting the financial system, while also fostering a secure, stable environment that supports industry growth. Establishing protocols and guidelines for risk management is therefore essential to promoting a resilient and compliant cryptocurrency ecosystem within the gambling industry.

SCOPE

This policy applies to all employees, contractors, and affiliates involved in the handling, processing, or management of cryptocurrency transactions within the Company. It encompasses all aspects of cryptocurrency operations, including deposits, withdrawals, and conversions.

COMPLIANCE AND REVIEW

The Compliance Officer will be responsible for ensuring adherence to this policy, conducting regular audits, and reporting compliance status to senior management.

2. RISK IDENTIFICATION AND ASSESSMENT

The identification and assessment of cryptocurrency risks require a thorough evaluation of the unique challenges these assets present, along with their potential impact on stakeholders. Cryptocurrencies are characterized by continuous innovation, with new blockchains, tokens, and decentralized platforms emerging rapidly. Monitoring and adapting to these changes is challenging, as new risks can arise unpredictably. This dynamic environment fragments the market, resulting in thousands of assets with distinct risk profiles. Assessing each—ranging from major coins like Bitcoin and Ethereum to smaller tokens—requires extensive resources due to their varying vulnerabilities and regulatory considerations. Limited historical data compared to traditional assets further complicates the development of reliable risk models.

The majority of crypto assets are traded on unregulated exchanges, where data quality and transparency are often limited. This can impair accurate asset assessments, potentially leading to misjudgments regarding asset reliability. Combined with high price volatility driven by speculative demand, market sentiment, and liquidity constraints, this poses a considerable risk for companies holding these assets.

Given these risks, the Company reserves the right to conduct additional background and security checks on clients depositing or withdrawing cryptocurrency. In cases of suspicion, the Company may suspend the account and request further documentation. Should the client's identity or funding source remain unverifiable, the matter is escalated to the Money Laundering Reporting Officer (MLRO) or management board, who may decide to terminate the relationship and secure any funds in a seized account. As a Curaçao GCB-licensed entity, the Company is obligated to report any unusual or suspicious transactions in accordance with the National Ordinance, and, as a registered entity with the Department of Financial Intelligence Unit (FIU), may submit a formal Suspicious Activity Report (SAR) if a client is linked to sanctioned activities, money laundering, terrorism financing, or other criminal behaviors.

Not lastly, the cryptocurrency landscape presents unique cybersecurity risks, including hacking, fraud, and smart contract vulnerabilities. To address this, the Company must maintain a high level of expertise in blockchain and cybersecurity. However, even stringent in-house security measures can be undermined by third-party vulnerabilities. Given the Company's reliance on external crypto exchanges, wallet providers, and other service providers, it conducts ongoing monitoring of these entities for derogatory actions or breaches. Assessing third-party risk is complex due to limited visibility into their internal controls, and this is further complicated by the lack of standardized risk assessment models in the industry.

To mitigate risks, the Company invests in employee training programs designed to enhance expertise and reduce the likelihood of misidentifying or miscalculating risks. Given the high stakes involved—such as loss of private keys or errors in wallet addresses—evaluating and managing the risks of operational errors is essential and requires robust internal controls and procedures.

Due to limited public understanding of cryptocurrency markets and their technical complexities, there remains widespread skepticism and an association with fraud, money laundering, terrorism financing, and regulatory evasion. The reputational risk associated with inadequate controls or compliance failures is difficult to quantify, but underestimating it can severely impact a company's reputation and operations.

In conclusion, the identification and assessment of cryptocurrency risks necessitate specialized knowledge, advanced analytical methods, and constant monitoring of evolving technological, regulatory, and market developments. Without a sophisticated approach, companies and investors face significant exposure to unexpected financial losses, compliance issues, and operational disruptions.

MITIGATION STRATEGIES

To mitigate risks in the cryptocurrency industry, the Company employs a set of comprehensive strategies.

First, it has established a robust compliance program, featuring rigorous Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols to verify customer identities and monitor for suspicious activity, thereby reducing the risk of financial crime. Additionally, the Company utilizes Chainalysis, a leading third-party crypto investigation tool, to enhance security and minimize risks associated with cryptocurrency transactions. To mitigate exposure to exchange rate fluctuations, the Company limits operations to the Tether stablecoin (TRC20 and ERC20).

A stringent internal control and risk management policy guides all cryptocurrency-related transactions. Employees follow standardized procedures for the review and approval of transfers, withdrawals, and fund allocations, significantly reducing the risk of operational errors.

The Company collaborates with experts in cryptocurrency and financial regulation to stay informed of evolving compliance standards. This proactive approach enables the Company to adjust policies promptly, maintaining alignment with regulatory requirements.

Employees participate in regular Cryptocurrency Handling and Security training, where they learn best practices for fraud prevention, regulatory compliance, and effective handling of crypto-specific risks. This ongoing education minimizes human error and strengthens internal security practices.

The Company does also employ multiple layers of cybersecurity protocols to protect digital assets and prevent unauthorized access. Cold storage is used to secure digital assets, while hot wallets hold only limited funds, reducing exposure to cyberattacks. Multi-factor authentication (MFA), encryption, and a complex access approval system provide additional security, safeguarding both funds and sensitive information.

The Company partners exclusively with reputable, well-established wallet providers, exchanges, and custodial services. Thorough due diligence is conducted to confirm that these partners' security practices meet industry standards and align with the Company's risk management policies.

Through these strategies, the Company seeks to mitigate key risks inherent to the cryptocurrency industry, including volatility, security threats, and regulatory uncertainties. This approach protects assets, strengthens operational resilience, and builds client trust.

CUSTOMER COMMUNICATION

The Company recognizes the importance of effective communication with clients regarding cryptocurrency-related inquiries. This approach is essential not only for building trust but also for ensuring client satisfaction and fostering loyalty. Clear and consistent communication enables clients to better understand the Company's products and services while facilitating efficient issue resolution. Clients can reach the Company through official communication channels listed on the website, including email and additional support options. This commitment to open communication enhances the client experience, strengthens the Company's reputation, and encourages long-term relationships, as clients who feel valued and supported are more likely to remain loyal and advocate for the business.

3. CONCLUSION

By adhering to this Crypto Risk Policy, the Company affirms its commitment to upholding the highest standards of security, regulatory compliance, and customer satisfaction across all cryptocurrency-related activities. All employees and stakeholders are expected to thoroughly understand and consistently apply the provisions of this policy. The primary advantages of this approach include elevated security standards and minimized financial risks. Through robust regulatory compliance, the Company fosters enhanced trust and confidence among both customers and employees. These practices safeguard assets, strengthen credibility, and ensure alignment with legal and industry standards.

4. RATIFICATION

The Policy will be valid for a period up to its annual or required reviewing.

In witness whereof, **Castianes B.V.** has caused this Policy to be duly executed this day of 20 of January 2025.

A handwritten signature in blue ink, appearing to be 'Annesol S.J. Melaria/Bryon J.A. Finies', is written over a horizontal line.

Annesol S.J. Melaria/Bryon J.A. Finies, Proxy-holder(s) of e-Management N.V. as
Director of Castianes B.V.