
Advanced Sports Entertainment N.V.
POLICY FOR CRYPTO USAGE

Approval

Version	Version Date	Approved By	Approval
1.0	July 2025	Director	

Abbreviations

“AML”	Anti Money Laundering
BRA	Business Risk Assessment
CAP	Customer Acceptance Policy
CTF	Counter Terrorist Financing
CDD	Customer Due Diligence
CFP	Counter Financing of Proliferation
CGA	Curaçao Gaming Authority
CRA	Customer Risk Assessment
EDD	Enhanced Due Diligence
FIU	Financial Intelligence Unit
KYC	Know Your Customer
MFA	Multi-Factor Authentication
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
UTR	Unusual Transaction Report
TF	Terrorist Financing

1. Introduction

1.1. Purpose

This policy establishes a standardized framework for managing risks associated with cryptocurrency use at Advanced Sports Entertainment B.V. (the “Company”). It is binding for all Company personnel, including directors, officers, employees, and relevant affiliates. The aim is to ensure financial, legal, and operational soundness while maintaining trust with clients.

Given the decentralized structure of cryptocurrencies, they are inherently vulnerable to misuse for unlawful activities such as ML, TF, and other financial crimes. As a licensed remote gaming operator, the Company bears the responsibility of enforcing stringent AML and CTF measures to prevent such abuse.

By implementing rigorous compliance protocols, the Company mitigates exposure to risk while offering a secure platform for clients. Enhanced transparency fosters user confidence and may promote broader cryptocurrency adoption. Cryptocurrencies also offer advantages such as lower transaction costs and faster processing times across international markets.

In the gambling sector, it is crucial to adopt a comprehensive policy that balances regulatory compliance, consumer protection, and operational efficiency. While digital assets present clear benefits, their risks must be proactively managed within a sound risk management structure.

Strong internal controls for cryptocurrency not only protect users and maintain financial integrity but also support sustainable growth in the sector. Establishing clear policies and risk oversight is vital to building a compliant and robust crypto ecosystem within the gaming industry.

1.2. Scope

This policy applies to all individuals and entities involved in the Company’s cryptocurrency transactions. It governs activities such as deposits, withdrawals, exchanges, and any operational function that involves digital assets.

1.3. Compliance and Review

The Compliance Officer is charged with monitoring adherence to this policy. Duties include conducting periodic audits and reporting compliance findings to the executive team.

2. Risk Identification and Assessment

Understanding crypto-related risks requires detailed analysis of evolving digital asset technologies and their potential impact on the Company and its stakeholders. The crypto sector is rapidly changing, with thousands of assets—ranging from leading tokens like Bitcoin and Ethereum to niche alternatives—each carrying unique risks and regulatory complexities.

A key challenge is the lack of oversight on many exchanges and the inconsistent quality of available data, making reliable risk evaluations difficult. Additionally, market volatility fuelled by speculation further increases the exposure of companies handling these assets.

In response, the Company reserves the right to apply Enhanced Due Diligence to any customer engaging in crypto transactions. Accounts may be temporarily restricted pending further documentation or clarification. If verification fails, the issue is escalated to the Compliance Officer (CO) or management, and a decision on account termination or fund retention is made. As required by Curaçao law, the Company files Unusual Transaction Reports UTRs with the FIU when criminal indicators are present.

Cryptocurrency use also introduces significant cybersecurity concerns, including hacking and fraud. Despite strong internal security protocols, external service providers may still present vulnerabilities. The Company therefore continuously monitors its crypto partners—wallets, exchanges, custodians—for signs of non-compliance or breaches.

Ongoing staff training in blockchain, cybersecurity, and AML risk is critical to improving risk recognition and reducing operational mistakes, such as wallet address errors or private key loss.

Given public misperceptions and regulatory scrutiny surrounding crypto, reputational risk must also be considered. Weak compliance could cause lasting damage to credibility and operations.

In sum, managing cryptocurrency risks requires expert analysis, vigilant oversight, and adaptation to emerging technologies, laws, and market dynamics. Failing to meet these standards may result in severe financial and operational repercussions.

2.1. Mitigation Strategies

To manage risks tied to crypto operations, the Company implements a multi-layered strategy:

2.1.1. Anti-Money Laundering Controls

A robust AML framework is in place, incorporating KYC procedures and continuous monitoring.

- In line with Curaçao regulations, CDD is required at or before any crypto transaction reaching Cg. 4,000. PEP and sanctions screening is mandatory during onboarding and thereafter.
- A Risk-Based Approach underpins Company operations. All crypto customers undergo a BRA and CRA. High-risk indicators, including mixing services or anonymizing tools, EDD, including documentation on source of funds and managerial approval.
- The Company retains all crypto-related transaction data for a minimum of five years and ensures availability to the CGA or FIU.
- Any new crypto tool or service is subject to a pre-adoption technological risk evaluation. This aligns with the Company's CAP, which defines criteria for declining or further assessing high-risk users.
- Standardized internal controls oversee all crypto transactions, minimizing human error and ensuring policy compliance.
- The Company maintains close collaboration with AML and crypto compliance specialists to track and respond to regulatory updates.
- Partnerships are limited to thoroughly vetted and reputable service providers, including exchanges and wallet platforms, whose controls match the Company's risk tolerance.

These controls help minimize volatility, operational disruptions, and regulatory violations while enhancing overall customer confidence.

2.1.2. Customer Communication

Transparent and responsive client communication is a core component of the Company's crypto compliance approach. Customers are provided clear guidance on digital asset usage, with access to official communication channels such as email and website-based support.

This transparency supports client satisfaction, strengthens loyalty, and enhances the Company's reputation in the marketplace

3. Conclusion

This policy underscores the Company's dedication to maintaining rigorous compliance and operational safeguards in its cryptocurrency-related activities. All stakeholders are expected to fully understand and uphold the principles outlined herein. Through comprehensive risk management and legal adherence, the Company enhances customer trust, protects assets, and ensures consistent alignment with regulatory expectations.