

CRYPTOCURRENCY SECURITY AND CONTROL POLICY

PR Entertainment N.V.

Effective Date: March 23, 2023

1. Purpose

This policy establishes the governance framework for the secure handling, storage, and operational use of cryptocurrency assets by PR Entertainment N.V., in compliance with Curaçao Gaming Authority (CGA) regulatory requirements.

2. Regulatory Alignment

PR Entertainment N.V. operates under the Curaçao gaming regulatory framework and ensures full adherence to AML, KYC, record-keeping, and transaction monitoring obligations applicable to cryptocurrency operations.

3. Governance Structure

A designated Responsible Officer oversees cryptocurrency systems. Oversight includes transaction authorization controls, wallet access management, regulatory reporting and incident escalation procedures.

4. AML, KYC and Transaction Monitoring

Client identification is required prior to withdrawal processing. Enhanced due diligence applies to high-risk accounts. All crypto transactions are screened through AML monitoring tools and retained for a minimum of five (5) years.

5. Wallet Management Controls

The majority of crypto holdings are maintained in cold storage. Hot wallets are limited to operational liquidity. Private keys are securely generated, encrypted and stored offline where feasible. Access is restricted and logged.

6. Security Framework

All wallet credentials and sensitive data are encrypted using industry-standard protocols. Multi-factor authentication (MFA) is mandatory. Access rights are role-based and reviewed periodically.

7. Transaction Authorization

Transactions exceeding predefined thresholds require multi-level approval or multi-signature validation. Exceptions require documented management approval.

8. Business Continuity and Incident Response

A Business Continuity Plan (BCP) addresses wallet compromise, cyber incidents, operational disruption, and disaster recovery. Incident reporting procedures include escalation to management and, where required, the CGA.

9. Training and Confidentiality

Personnel involved in crypto operations receive ongoing compliance and security training. Confidentiality agreements are mandatory.

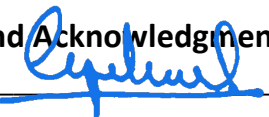
10. Policy Review

This policy is reviewed annually or upon regulatory changes. Updates require senior management approval and documented version control.

11. Non-Compliance

Violations may result in disciplinary measures, termination, and regulatory reporting where legally required.

Approval and Acknowledgment

Approved by:  _____

Name: Maya Baroud

Title: Managing Director

Date: February 1, 2026