

Bridge Technologies B.V

Know Your Customer (KYC) Policy

Version 1.0

January 2025

Table of Contents

1. Purpose and Scope	3
2. Regulatory Framework.....	3
3. KYC Objectives	3
4. Customer Identification and Verification.....	3
5. Ongoing Monitoring	4
6. Enhanced Due Diligence (EDD).....	4
7. Record Keeping.....	4
8. Data Protection.....	5
9. Sanctions and PEP Screening.....	5
10. Responsibilities.....	5
11. Non-Compliance and Account Restrictions.....	5
12. Review and Updates	5
Document Control.....	6
Document Classification.....	6

1. Purpose and Scope

This KYC Policy outlines the procedures and controls implemented by Bridge Technologies B.V. (“the Company”) to identify and verify the identity of its players/customers in accordance with Curaçao’s Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regulatory framework. The policy applies to all individual players who register and transact on the Company’s platform, including deposits, withdrawals, and gameplay activities.

2. Regulatory Framework

This Policy is developed in line with:

- The National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NORUT);
- The Guidelines issued by the Curaçao Gaming Control Board (GCB);
- FATF Recommendations (Financial Action Task Force);
- Internal AML/CFT Policy and Risk Assessment of Bridge Technologies B.V.

3. KYC Objectives

The primary objectives of this Policy are to:

- Verify the identity of players prior to allowing access to the platform;
- Prevent the use of the Company’s services for money laundering, terrorist financing, or fraud;
- Ensure compliance with Curaçao AML/CFT laws and GCB licensing conditions;
- Maintain transparent and traceable player records;
- Enable risk-based monitoring of player activity.

4. Customer Identification and Verification

KYC verification is mandatory when:

- A player registers an account;
- A player deposits or withdraws funds;
- Cumulative transactions reach or exceed USD 2,000 (or equivalent);
- Suspicious or unusual activity is detected;
- There is doubt about the veracity or adequacy of previously obtained documents.

Minimum identification requirements:

- Full Legal Name

- Date of Birth (must be 18+)
- Residential Address
- Valid Email Address
- Government-Issued Photo ID (passport, national ID card, or driver's license)

Verification procedures include document validation, proof of address verification, and optional face verification. Cryptocurrency users must verify wallet ownership and source of funds.

5. Ongoing Monitoring

Continuous transaction and gameplay monitoring is performed to detect unusual or inconsistent activity.

Enhanced Due Diligence (EDD) is applied to higher-risk players or transactions.

Withdrawals may be delayed pending successful re-verification.

6. Enhanced Due Diligence (EDD)

EDD measures apply to:

- Politically Exposed Persons (PEPs);
- Players from high-risk jurisdictions;
- High-value or rapid transactions;
- Players using cryptocurrency for deposits or withdrawals.

Additional documentation may include:

- Source of Funds (SoF);
- Source of Wealth (SoW);
- Verification of crypto wallet ownership.

7. Record Keeping

All KYC documentation, transaction records, and crypto transaction data are securely stored for a minimum of 5 years after account closure or last transaction.

Records must be accessible to the MLRO, Compliance, and regulators upon request.

8. Data Protection

Player data is handled in compliance with GDPR and Curaçao data protection laws and used solely for AML/CFT compliance and operational purposes.

9. Sanctions and PEP Screening

All players are screened against UN, EU, OFAC, and local sanctions lists.

PEP and sanctions screening is automated and repeated regularly.

10. Responsibilities

The Compliance Officer / MLRO oversees KYC procedures.

Customer Support and Payments Teams ensure timely player verification.

All staff receive regular AML/KYC training and report suspicious activity to the MLRO.

11. Non-Compliance and Account Restrictions

Failure by a player to provide satisfactory KYC documentation or clarification may result in:

- Account suspension or restriction;
- Blocking of deposits or withdrawals;
- Reporting to the Financial Intelligence Unit (FIU Curaçao).

12. Review and Updates

This Policy shall be reviewed annually or upon material changes in Curaçao AML/CFT legislation, FATF guidance, or internal risk assessments.

Approved by:

Board of Directors
Bridge Technologies B.V
Curaçao

Effective Date: 10/01/2025**Next Review Date:** 10/01/2026**Document Control**

Version	Date Approved	Approved By	Next Review Date	Status
1.0	10/01/2025	Board of Directors	10/01/2026	Active

Document Classification**Confidential – Internal / Regulatory Use Only**

This document contains proprietary and confidential information belonging to Bridge Technologies B.V. It may not be copied, distributed, or disclosed without prior written authorisation from the Company or the Curaçao Gaming Control Board.