



BetU Curaçao B.V.

AML-CTF Policy and Procedures.

CONTENTS

1 Version Control.....	3
2 Document Details.....	4
2.1 Process Name.....	4
2.2 Objective/Goal.....	4
2.3 Description.....	4
2.4 Parent Process.....	4
2.5 Ownership.....	5
3 AML-CTF Brief.....	6
Item 1: Introduction.....	6
Item 2: Money Laundering Defined.....	6
Item 3: Terrorist Financing Defined.....	6
Item 4: Curaçao Gaming Control Board (GCB) Requirements.....	7
Item 5: Accountability and Commitment.....	7
Item 6: Immunity From Prosecution.....	8
Item 7: Risk-Based Approach.....	8
Item 8: Risk Mitigation.....	9
Item 9: Training.....	9
Item 10: Review of the Program.....	9
Item 11: Record Keeping.....	10
Item 12: Client Intake and Authentication.....	10
Item 13: Politically Exposed Persons.....	11
Item 14: Transaction Records.....	11
Item 15: Monitoring.....	11
4 Next Update.....	12

1 VERSION CONTROL

Version	Version Description	Author	Reviewer	Date Approved	Description
1.0	Creation of Policy	BetU Curaçao B.V Compliance		27-FEB-2024	Initial Creation of Document
2.0	Major updates	Phantom Compliance		07-AUG-2024	Major updates and review, major formatting updates.

2 DOCUMENT DETAILS

2.1 PROCESS NAME

AML-CTF Policy contains:

- Business Model Brief
- AML/CTF Brief
- Curaçao Gaming Control Board Requirements
- Risk Assessment
- Record Keeping
- Client Intake and Politically Exposed Persons
- Monitoring

2.2 OBJECTIVE/GOAL

The document's objective is to outline the requirements for compliance with the Curaçao Gaming Control Board and the Department of the Financial Intelligence Unit (FIU). Risks are assessed, strategies to mitigate, transfer, and avoid are outlined, and additional aspects of the compliance regime are summarized.

Standards set out in this AML and KYC policy/procedures documents are based on applicable legal and regulatory requirements, especially on the EU AML directive (Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) to effectively prevent any money laundering, terrorist financing or other fraudulent activities.

2.3 DESCRIPTION

This document provides an internal/external reference for staff and partners to consult anytime.

BetU Curaçao B.V is committed to the highest ethical standards regarding anti-money laundering (AML) and countering the financing of terrorism (CFT) consistent with International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation”.

This AML/CFT Policy (the Policy) aims to safeguard BetU Curaçao B.V against money laundering (ML) and the financing of terrorism (FT or TF) risks. The Policy outlines the principles and minimum standards of internal AML/CFT controls that should be adhered to by BetU Curaçao B.V to mitigate reputational, regulatory, legal, and financial loss risks.

2.4 PARENT PROCESS

None.

2.5 OWNERSHIP

	Primary	Secondary
Name	Ryan Mueller	
Designation	Chief Compliance Officer	
Department	Phantom Compliance	
Email	ryan@phantomcompliance.com	

3 AML-CTF BRIEF

ITEM 1: INTRODUCTION

- BetU Curaçao B.V is a company registered and incorporated in Curaçao with Company registration: 158488. It is licensed and regulated by the Government of Curaçao under the gaming license 1668/JAZ issued by Curaçao eGaming and operates the website www.ubet.io.

ITEM 2: MONEY LAUNDERING DEFINED

- Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets.
- There are 3 “typical” stages in the process:
 - **Placement** – initial deposit of proceeds of crime into the financial system, placement may or may not include the predicate offense from which illicit funds were derived.
 - **Layering** – conducting multiple transactions and/or transfers to convert illicit funds to another form and obfuscate the true source/original placement.
 - Layering may include transferring the value from one vehicle/object to another including the purchase of high value assets (jewelry, vehicles, property) and multiple money transfers from one instrument to another (money orders, checks, bearer bonds, prepaid cards, etc.)
 - Multiple BTC or other crypto transactions between related wallets is a perfect example of layering.
 - **Integration** – withdrawal or conversion of the funds to a “clean” form, typically this includes “fencing” stolen or illicitly obtained goods for comparable value, this could be selling bitcoin for cash or wire or reselling stolen goods for cash.
- Money laundering may, or may not be, accompanied by a predicate criminal offense.
 - A simple money laundering scheme may involve using a stolen financial instrument to purchase a high-value item intended for resale, in this case, theft of the financial instrument precedes the use/attempted conversion of the same.
 - A more complex scheme could involve the purchase of multiple prepaid cards followed by fictitious purchases with the cards to a shell merchant to receive the funds via a commercial settlement payment.
- Concerning BetU Curaçao B.V the largest money laundering risks lie in criminals seeking to engage in Gaming activities via the use of crypto to place and layer illicit funds in the legitimate economy, criminals conducting illicit gaming transactions on behalf of themselves or an undisclosed third party, or criminals using stolen identities/financial instruments to engage in online gaming.

ITEM 3: TERRORIST FINANCING DEFINED

- Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations.
- Funds may be sourced from a variety of sources including donations, real business activities, AND criminal sources such as drug/human trafficking and other illicit industries.
- The movement of funds for terrorist financing often mimics that of money laundering in that one, or more, of the points at which the funds enter/exit the financial system is being intentionally obfuscated.

ITEM 4: CURAÇAO GAMING CONTROL BOARD (GCB) REQUIREMENTS

The Curaçao Gaming Control Board (GCB) imposes stringent Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) requirements on licensed operators. These requirements align with international standards to prevent money laundering and terrorist financing activities.

Know Your Customer (KYC) Procedures:

- Customer Identification: BetU Curaçao B.V verifies the identity of customers before establishing a business relationship or allowing significant transactions.
- Ongoing Monitoring: BetU Curaçao B.V continuously monitors customer activities to identify unusual or suspicious transactions.

Record-Keeping:

- Transaction Records: BetU Curaçao B.V maintains records of all transactions for at least five years.
- Customer Information: BetU Curaçao B.V keeps detailed records of customer identification and verification processes.

Suspicious Transaction Reporting:

- Reporting Obligations: BetU Curaçao B.V will report any suspicious transactions to the Financial Intelligence Unit (FIU) of Curaçao.
- Threshold Reporting: BetU Curaçao B.V will report large transactions that exceed specific thresholds, even if they do not appear suspicious.

Risk Assessment:

- Risk-Based Approach: Implement a risk-based approach to identify, assess, and mitigate money laundering and terrorist financing risks.
- Enhanced Due Diligence: Apply enhanced due diligence measures for higher-risk customers and transactions.

Internal Controls and Procedures:

- Compliance Program: Establish and maintain an effective AML/CTF compliance program, including policies, procedures, and controls.
- Training: Provide ongoing training for staff on AML/CTF policies and procedures.

Independent Audits:

- Regular Audits: BetU Curaçao B.V conducts independent audits of the AML/CTF program to ensure its effectiveness and compliance with regulations.

Reporting and Cooperation:

- Regulatory Reporting: We regularly report to the GCB and other relevant authorities on compliance status.
- Cooperation: Cooperate with regulatory authorities during inspections and investigations.

Customer Due Diligence (CDD):

- Standard CDD: BetU Curaçao B.V will conduct standard due diligence on all customers.
- Simplified and Enhanced CDD: Apply simplified or enhanced due diligence measures as appropriate based on the risk assessment.

ITEM 5: ACCOUNTABILITY AND COMMITMENT

- BetU Curaçao B.V is committed to deterring and combating money laundering/terrorist financing in our systems and the world at large.
- BetU Curaçao B.V has adopted a risk-based approach and compliance strategy that is approved by the management.

- Per this policy, as a part of the company's Compliance Program, BetU Curaçao B.V is committed to full compliance with requirements that are designed to deter and detect actual/potential money laundering/terrorist financing (ML/TF) as well as other activities that enable/facilitate OR are related to ML/TF.
- BetU Curaçao B.V encourages and actively develops an internal culture of compliance and ethics among staff, see other policies for details.
- BetU Curaçao B.V dedicates resources to compliance and risk management including implementing the below recommendations from Curaçao Gaming Control Board for a sufficient compliance regime:
 - Monitoring the risk assessment of the firm against ML/TF occurring in the daily activities
 - Instituting and documenting the ongoing compliance training program for all BetU Curaçao B.V staff, agents mandataries, or other authorized persons.
 - Development and application of internal policies, processes, and other initiatives directly related to anti-money laundering/counter-terrorist financing.
 - Regularly scheduled independent reviews to assess the efficacy and relevance of the Compliance program.

ITEM 6: IMMUNITY FROM PROSECUTION

- BetU Curaçao B.V recognizes that part of any effective compliance function is protection for those who comply or attempt to comply in good faith.
- BetU Curaçao B.V supports the requirement for personnel to identify and report suspicious or otherwise reportable transactions to Curaçao Gaming Control Board and will attempt to protect staff from civil and criminal proceedings where possible.

ITEM 7: RISK-BASED APPROACH

- BetU Curaçao B.V employs a risk-based approach (RBA) and therefore development and implementation of the compliance program are informed by the risk appetite of BetU Curaçao B.V and its strategic partners according to the company's RBA.
- In the context of ML/TF, risk has two meanings:
 1. National level, and
 2. Company/Reporting Entity level. Regarding the company level, we have internal and external threats and vulnerabilities that could expose the company to being used to facilitate ML/TF activities.
- **Threats:** A person, group, or object that could cause harm. In the ML/TF context, threats could be criminals, third parties facilitating ML/TF, terrorists, or terrorist groups or their funds.
- **Vulnerabilities:** Elements of a business or its processes that are susceptible to harm and could be exploited by a threat. In the ML/TF context, vulnerabilities could include weak business controls or high-risk services.
- Following regulations the Compliance team monitors risk assessments through RBA specifically related to ML/TF risks.
- Incident to the RBA the Compliance team makes and implements recommendations to diminish the risk to an acceptable level.
- Where risk cannot be sufficiently mitigated/transferred/avoided BetU Curaçao B.V may decline to engage in the risky activity.

ITEM 8: RISK MITIGATION

- It is BetU Curaçao B.V policy to conduct due diligence via the customer intake process on all clients regardless of their risk profile.

Individual Customers

1. The Curaçao Gaming Control Board (GCB) provides detailed guidance on client identification to ensure compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations. Here are the key aspects of their guidance on client identification:

Customer Identification Program (CIP):

- Verification: Verify the identity of customers using reliable, independent source documents, data, or information.
- Timing: Perform identification and verification before establishing a business relationship or conducting transactions above a certain threshold.

Required Information:**For Individuals:**

- o Full name
- o Date of birth
- o Nationality
- o Residential address
- o Identification document details (e.g., passport, national ID card)

For Legal Entities:

- o Legal name
- o Business address
- o Registration or incorporation number
- o Names of directors and beneficial owners
- o Nature and purpose of the business relationship

Document Verification:

- o Primary Documents: Use government-issued identification documents, such as passports, national ID cards, or driver's licenses.
- o Secondary Documents: Supplement primary documents with secondary documents, such as utility bills, bank statements, or other proof of address.

ITEM 9: TRAINING

- BetU Curaçao B.V has implemented, and maintains, an ongoing AML-CTF training program to ensure all staff are familiar with their Money Laundering and Terrorist Financing obligations.
- At a minimum, all staff are required to complete this training within 30 days from being hired AND once annually subsequently.

ITEM 10: REVIEW OF THE PROGRAM

- BetU Curaçao B.V shall facilitate regular independent reviews of their AML-CTF regime by qualified auditors when required by Curaçao Gaming Control Board guidelines.
- This review will assess internal control, transaction processing systems, and procedures.
- Where issues/deficiencies are identified, BetU Curaçao B.V will endeavor to remediate them in a timely fashion.

- A report of any completed audit will be retained for a minimum of 5 years and contain:
 - Description of the review's scope
 - Review of policies and procedures
 - Review of the current training program
 - Assessment of intake, record keeping, identity verification, and other processes to ensure they are commensurate with Curaçao Gaming Control Board guidance
 - Summary of any deficiencies
 - General findings

ITEM 11: RECORD KEEPING

- BetU Curaçao B.V complies with the record keeping requirements delineated by the Curaçao Gaming Control Board. The following records will be maintained:
 - Regulatory filings – a copy of all reports submitted to the Curaçao Gaming Control Board and the Department of the Financial Intelligence Unit (FIU)
 - Suspicious Transaction Reports.
- Reports are stored for a minimum of 5 years.
- Policies and procedures are kept up to date (several factors could trigger the need to update, such as changes in legislation, non-compliance issues, new services or products, or the two-year effectiveness review). Updates are tracked by the Last Updated tag and by Policy Version Number.

ITEM 12: CLIENT INTAKE AND AUTHENTICATION

- BetU Curaçao B.V primary clients are individuals.
- BetU Curaçao B.V offers services to clients in an online/non face to face fashion
- The customer intake procedure applies to all clients regardless of application method and is guided by global standards.
- Where dictated by risk level additional due diligence may apply.
- Executive management approval is a compulsory requirement for onboarding high-risk clients.
- Individuals verify through [Onfido](#) and provide:
 - Date of birth.
 - Government-issued identification.
 - Proof of address document.
 - Occupation.
 - Liveness verification.
- Individuals are allowed to self-report if are politically exposed persons.
- Using [Onfido](#) entity names and individuals are checked against multiple watch lists including the [OFAC SDN list](#).
 - Where a possible match is identified additional information will be requested from the client and enhanced due diligence conducted.
 - BetU Curaçao B.V does not knowingly transact with excluded parties.
 - Positive matches will be denied service, all other outcomes result in enhanced due diligence and monitoring.

ITEM 13: POLITICALLY EXPOSED PERSONS

- BetU Curaçao B.V takes reasonable measures to independently determine if a client is designated as a:
 - Politically exposed person (PEP)
 - Politically exposed foreign person (PEFP)
 - A relative or close associate of a PEP/PEFP (RCA)
- These measures apply to the following scenarios:
 - New client intake
 - New customers making high-value stakes.
- Where a transaction/group of transactions is suspected to have been conducted by a PEP/PEFP/RCA the transaction is reviewed with attention to:
 - Is the customer name a match to the OSFI/OFAC/UN/EU watch lists?
 - Can the customer's identity be validated by public records or social media?
 - Does the purchase size make sense?
 - Where is the customer located? Where is the merchant located?
 - What payment instrument was used for the transaction? Is this a high-risk payment instrument?
- If the customer is deemed to be a PEP/PEFP/RCA a record of the transaction will be prepared within 14 calendar days including:
 - Office or position of the customer/client
 - Source of funds/wealth/VC (if known)
 - Date PEP/PEFP/RCA status confirmed
 - Source used to confirm client/customer status
 - Name of staff member who completed the review
 - Date the transaction(s) was reviewed
- PEP activity will be reviewed on an ongoing basis to ensure risk is managed accordingly

ITEM 14: TRANSACTION RECORDS

- BetU Curaçao B.V stores an electronic record of all transactions processed through our systems regardless of type, status, or amount.
- All transaction records are stored for a minimum of 5 years per Curaçao Gaming Control Board guidelines and will be stored for the lifetime of the BetU Curaçao B.V business unless a client/customer specifically requests the deletion of their information per the terms governing privacy and consent in their jurisdiction
- Any questions regarding the destruction of records can be directed to BetU Curaçao B.V.com

ITEM 15: MONITORING

- BetU Curaçao B.V reviews transactions daily to ensure if presented with a risk of money laundering or terrorist financing based on location or amount is reviewed in full.
- Enhanced due diligence is conducted on clients that transact in high volumes every day via internal reporting and operational procedures.
- High volume/high velocity transfers from customers are reviewed weekly by our Risk team.
- Ongoing monitoring for sanction, PEP, and adverse media is conducted by [Onfido](#) with daily alert checks conducted by Compliance.
- Compliance reviews client's transactions for the following reasons:

- o To ensure transactions that present a risk of money laundering or terrorist financing based on client occupation or amount are reviewed in full.
- o To determine a customer profile – review transactions to gauge if there is a change in the customer risk profile.
- o To monitor ongoing sanction screening to ensure sanctioned and excluded parties are not serviced.
- o To flag high-value transactions and determine their legitimacy.
- o To monitor for PEPs that may be active.

4 NEXT UPDATE

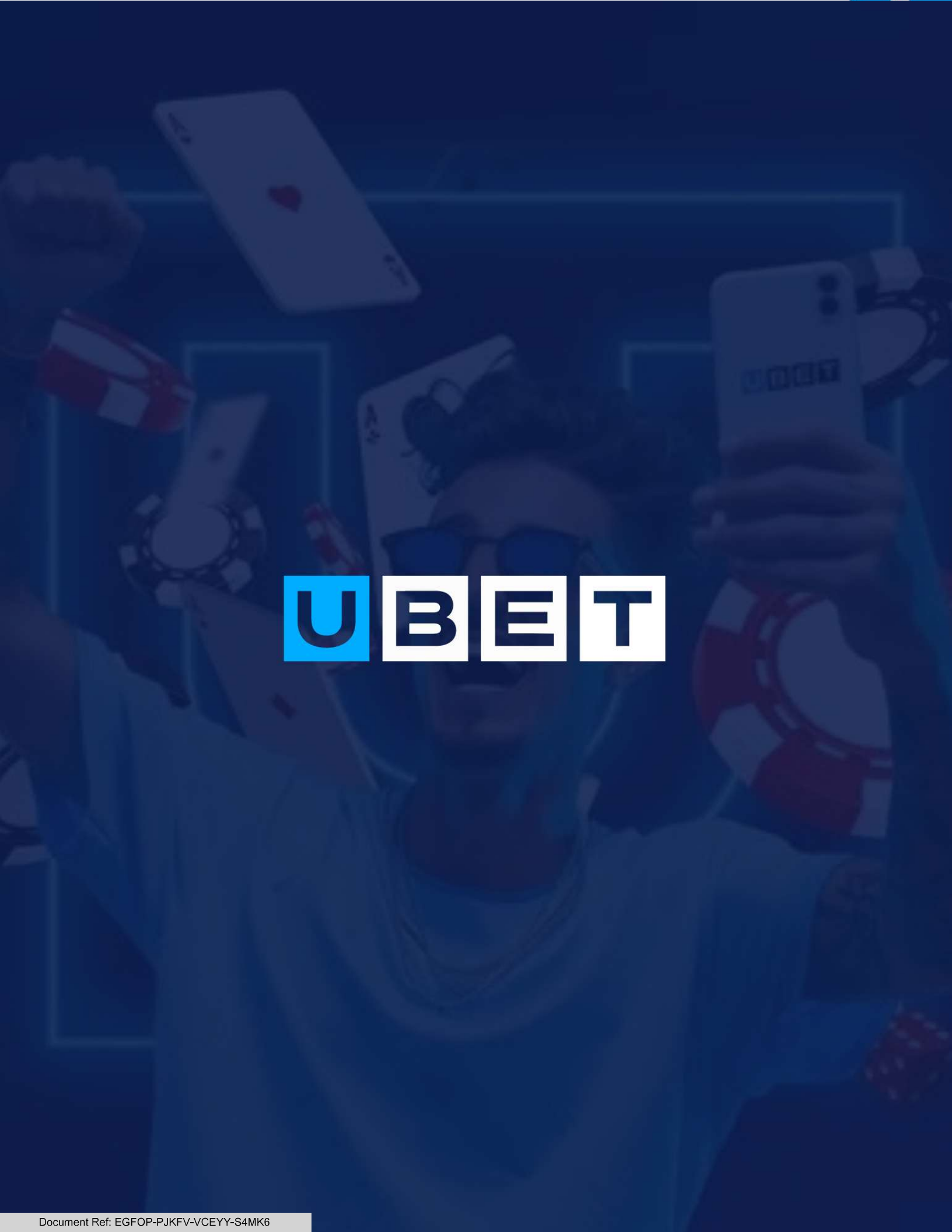
- August 2025

Peter Lawrence

Signature

2024-08-19

date

A person with curly hair and sunglasses is smiling and celebrating. They are holding a smartphone in their right hand, which has a 'UBET' sticker on the back. Several playing cards, including an Ace of Hearts and an Ace of Spades, are floating in the air around them. They are also holding a red and white striped object, possibly a party horn or a small flag. The background is a dark blue grid pattern.

UBET

Signature Certificate

Reference number: EGFOP-PJKFV-VCEYY-S4MK6

Signer

Timestamp

Signature

Peter Lawrence

Email: peter.lawrence@saintlyholdings.com

Sent:

16 Aug 2024 17:57:41 UTC

Viewed:

16 Aug 2024 17:58:13 UTC

Signed:

19 Aug 2024 00:03:30 UTC

Peter Lawrence

Recipient Verification:

✓ Email verified

16 Aug 2024 17:58:13 UTC

IP address: 1.145.113.164

Location: Sydney, Australia

Document completed by all parties on:

19 Aug 2024 00:03:30 UTC

Page 1 of 1



Signed with PandaDoc

PandaDoc is a document workflow and certified eSignature solution trusted by 50,000+ companies worldwide.

