



**Anti-Money Laundering (AML) / Combatting Financing of Terrorism (CFT) and
Combatting of Proliferation (CFP) Policy**

June 2025

Prepared by :

Jack's House B.V. (d/b/a Otherworld.xyz)

Emancipatie Boulevard Dominico F. "Don" Martina 31
Curaçao

Two handwritten signatures in blue ink, one above the other, positioned over the "CONFIDENTIAL" watermark.

e-Management N.V.
Director

Contents

1. Introduction	3
2. Policy Statement	3
2.1 Purpose of this Policy	4
3. Introduction	5
3.1 Background	5
3.2 Objectives and Scope	5
3.3 Applicability	6
3.4 Document Updates	6
3.5 Disclaimer	6
4. The Risk-Based Approach	7
4.1 Explanation of the Risk-Based Approach	7
4.2 Business Risk Assessment	7
5. Customer Acceptance Policy	7
5.1 Customer Risk Assessment	7
Customer Risk	7
5.2 Product/Service Risk:	8
5.3 Geographic Risk:	8
5.4 Delivery Channel Risk:	9
5.5 Prohibited Accounts	9
6. Governance Framework	10
7. AML Framework	11
7.1 The AML Policy	12
7.2 Targeted Financial Sanctions	15
7.3 Politically Exposed Persons (PEPs)	16
7.2 Monitoring	17
8. Collusion and Cheating	19
9. Reporting of unusual transactions	19
9.1 Recognition of unusual transactions	19
9.2 Prohibition of disclosure	20
10. AML/CFT/CFP Training Program	20
11. Record Keeping	22
12. Audit	22
13. Appointment of a Compliance Officer	23
13.1 Duties of the AMLO	23
Appendix I: Country Risk List	24
Appendix II: Business Affiliate and Supplier Due Diligence	26
Appendix III: Internal Unusual Activity Report	27

1. Introduction

Otherworld is the online casino brand of Jack's House B.V., a company based in Curaçao that holds a Curaçao gaming license. To keep the platform safe and fair, we take strong steps to prevent money laundering, the financing of terrorism and proliferation which is when people try to hide illegally obtained money by making it look legitimate. Our goal is to ensure that Otherworld is not used for illegal activities while maintaining a secure and enjoyable gaming experience for all players.

How We Prevent Money Laundering the financing of terrorism and proliferation

1. **Verifying Players Before They Play**
 - a. Every new player must register with their real name, address, date of birth, and email.
 - b. We verify each player's identity using official documents like passports or driver's licenses.
 - c. Players must confirm their email before their account is activated.
 - d. We do not allow anyone under 18 years old to play.
2. **Monitoring Player Transactions.** We track deposits, withdrawals, and betting activity for unusual patterns.
3. **Blocking Suspicious Accounts**
 - a. If we find that an account may be involved in illegal activity, we freeze the funds and report the case to authorities if necessary.
 - b. Players who try to cheat, collude, or manipulate the system will be banned from the platform.
4. **Training Our Employees**
 - a. Our staff is trained to recognize suspicious activities and report them immediately.
 - b. Every employee understands that they cannot warn a player if their transactions are being investigated.
5. **Keeping Records and Updating Policies**
 - a. We store all verification documents and player transaction histories for at least five years.
 - b. Our Anti-Money Laundering Officer (AMLO) updates this policy to stay in line with new regulations and best practices.

2. Policy Statement

Jack's House B.V (hereinafter "Otherworld" or the "Company"), is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games on the internet. In accordance with the license conditions, Jack's House B.V. has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (hereinafter "AML, CTF and CPF") policy (hereinafter the "Policy").

As a responsible gaming enterprise operating in Curaçao, Company Name acknowledges the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

2.1 Purpose of this Policy

The purpose of this Policy is to ensure the Company's compliance with the relevant legal and regulatory requirements from the authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector are the CGA and the Curaçao Financial Intelligence Unit (FIU), while simultaneously ensuring the integrity and sustainability of the operations of the Company.

The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);

Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025

3. Introduction

3.1 Background

Money laundering is defined as the process of covering up or “laundering” illegally obtained money to wipe away traces of criminal activity and make it appear as if it were legitimately obtained. The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, and the legislative/regulatory/law enforcement environment of the market in which the money launderer operates. Since e-commerce and online gambling platforms can be used for money laundering (“ML”) purposes, they face reputational, legal, and regulatory risks. Many companies invest large amounts of time and money to develop their business, and their reputation invariably takes years to build. However, this can be lost in an unbelievably short time if the organization becomes embroiled in an ML scandal.

Terrorism Financing (TF) refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Unlike ML, which always involves proceeds from illegal activities, terrorist financing may not necessarily derive from illicit sources; instead, it often utilizes legitimate funds from charitable donations, business profits, or foreign government sponsorships. While both terrorism financing and money laundering may employ similar methods – such as cash smuggling, structuring, wire transfers, and the use of debit and credit cards – the primary concern of TF is to obscure the intended use or end recipient of the funds rather than their origin. Additionally, funding for terrorist activities does not always require large sums of money, as it can accumulate over time through simple transactions.

Therefore, the Company is implementing measures to ensure that money gained through unlawful means is not channeled and laundered through the Company’s platform.

3.2 Objectives and Scope

This Anti-Money Laundering (“AML”) Policy (the “Policy”) is intended to define the policies and procedures implemented by the Company to prevent and effectively combat ML. By appropriately implementing this Policy, Jack’s House will ensure that the users of its platform do not expose the Company to regulatory risks. To this end, Jack’s House and its employees who interact with customers should be aware and appropriately trained on how to recognize and address transactions and other activities that may be related to ML.

Accordingly, the objectives of this Policy are the following:

- To raise the level of knowledge on ML and the manner in which the Company’s products and services could be exploited to facilitate ML;
- To provide awareness of the Company’s AML Policy designed to assist in the detection, prevention, and deterrence of potential ML activities;
- To provide a reference to employees of the procedures developed by the Company in relation to the implementation of its AML Policy and its legal obligations; and
- To effectively combat ML and mitigate reputational and regulatory risks arising from ML activities.

3.3 Applicability

Jack's House is committed to identifying and mitigating ML risks emanating from its products and services. Thus, adherence to the provisions of this Policy is critical to the effective implementation of the AML program developed by the Company. Therefore, this Policy is applicable to Senior Management and all employees of the Company. Additionally, every newly onboarded employee is required to read this Policy and undergo the appropriate AML training. This Policy will also be made accessible to all employees upon request. In addition, the Company may offer periodic training to review the Policy.

The Company aims to attain company-wide awareness of Jack's House's AML obligations along with an effective level of regulatory compliance commensurate with the nature and size of the business. The procedures and measures outlined herein are tailored for a remote gaming business like the platform offered by the Company.

3.4 Document Updates

This document will be revised to reflect, as applicable, any regulatory updates and changes to internal procedures. The Company will identify an Anti-Money Laundering Officer ("AMLO") who will be responsible for facilitating any updates to the Policy and reviewing it regularly to ensure the Policy remains relevant to changing business and regulatory requirements. New versions of this Policy will be given a version number in the following manner "AML Policy V1.0" and saved for access to all employees.

Details regarding revised versions will be documented in the "Version Control" table preceding the Introduction of this Policy. Any material changes to the Policy will be communicated to all employees via email.

3.5 Disclaimer

The information contained in this Policy is confidential and for internal use only. However, the contents of this Policy may be shared with third parties (e.g., legal counsel) as appropriate.

4. The Risk-Based Approach

4.1 Explanation of the Risk-Based Approach

Company Name adopts a risk-based approach in our AML compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF/PF risks specific to the online gaming industry. When developing its AML compliance program, the Company assesses risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Company may employ simplified measures.

To effectively apply the risk-based approach, the Company conducts a preliminary assessment of the risks associated with money laundering and terrorist financing within the organization, and based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

Company Name shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. Company Name shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

4.2 Business Risk Assessment

The Business Risk Assessment (BRA) framework is a crucial component of Company Name's AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating money laundering, terrorist financing, and proliferation financing risks within the Company's operations.

Company Name performs thorough BRAs, evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed regularly. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment.

5. Customer Acceptance Policy

5.1 Customer Risk Assessment

The Customer Risk Assessment assesses the particular risks the Company will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. The determination of the Customer Risk Rating is first assigned when a new customer applies for an account. This rating helps decide how often and in what way the customer will be reviewed in the future: the higher the risk, the more frequent and robust the ongoing monitoring of the customer would be.

The Customer Risk Assessment process takes into consideration the following factors:

Customer Risk

This involves assessing the customer's background, occupation, and transaction patterns. Categories of customers whose activities indicate a higher risk include:

- Customers who have multiple sources of income;

- Customers with irregular income streams;
- PEPs;
- High spenders;
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures.

5.2 Product/Service Risk:

This factor evaluates the risks associated with the products and services offered, including gaming products or services where customers can influence game outcomes, either on their own or in collaboration with others. Additionally, certain payment methods used by customers and accepted by casinos are seen as riskier for ML and TF. The following is a non-exhaustive list of high-risk factors:

- Anonymous payment methods (e.g. pre-paid cards and virtual assets);
- Unusual casino account usage;
- Specific game types, where bets are made even;
- Peer-to-peer gaming;
- Third-party accounts;
- Moving money from one gaming account to another;
- Multiple accounts or wallets;
- Additions or changes to associated payment methods.
- Identity fraud: Stolen financial account details used on websites, including stolen identities used to open financial accounts that are then used for gambling.
- Games with multiple operators: For example, poker platforms shared by different operators.
- Electronic wallets: Not all e-wallets are licensed in trustworthy countries, and some accept cash deposits. Moreover, e-wallets that only accept funds from financial accounts may not show the transaction to the online casino, which could help dishonest customers hide their gambling activities.

5.3 Geographic Risk:

This assessment considers the geographic location of the customer and the transaction, with countries that have weak AML, CTF and CPF regulations or high levels of corruption being deemed higher risk. The nationality, residence and place of birth of the player have to be considered as these might be indicative of a heightened geographical risk. Company Name regards the following sources of information produced by the FATF and other well-known non-governmental bodies (not limited):

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML, CTF and CPF regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

Company Name consistently monitors updates to the lists above and adjusts its CDD process to reflect relevant changes. Please see [Appendix I](#).

5.4 Delivery Channel Risk:

This factor looks at the risks associated with the methods used to establish a business relationship or through which transactions are carried out. Company Name considers the increased risk of ML/TF/PF of the use of channels that favor anonymity and interactions on a non-face-to-face basis and, to the extent possible, shall take all reasonable measures to address and mitigate said risks.

The risk assessment will categorize customers as low, medium, or high risk, with due diligence and ongoing monitoring applied proportionately:

- For customers assessed as low risk, the Simplified Due Diligence process will be applied, insofar as the customer does not display any risk-increasing elements and remains below the threshold of NAf. 4,000.
- For those assessed as medium or high risk, additional information and documentation will be required in accordance with this Policy.
- Accounts classified as high risk or exhibiting potentially suspicious behaviors will be subject to review by compliance personnel and reported to the Compliance Officer (CO) for further investigation.

5.5 Prohibited Accounts

Company Name's Customer Acceptance Policy is formulated in accordance with legal requirements and aligns with the Company's risk appetite as well as the BRA. Therefore, certain categories of individuals are prohibited from being accepted as customers, either by preventing them from registering or by blocking their access to our site, as necessary:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by UN, EU or OFAC.
- Individuals for whom there are reasonable grounds to suspect involvement in ML/TF/PF or any other form of criminal activity.
- Self-excluded customers who are barred from our websites or included in any national self-exclusion registers as stipulated by licensing conditions.
- Individuals who have submitted documents or information that the Company has reasonable grounds to suspect are fraudulent or falsified.

6. Governance Framework

The Company has implemented an AML framework that encompasses appropriate governance and oversight roles, internal controls, and sound practices for the management and supervision of the risks associated with ML.

a. Senior Management Responsibility

Senior Management of the company will remain fully engaged in the implementation of this Policy. Accordingly, Senior Management will ensure that the Company is equipped with the requisite resources to carry out this Policy. Additionally, Senior Management will assist the AMLO in updating this Policy as necessary to ensure compliance with relevant regulatory obligations.

b. AML Officer

The Chief Legal Officer has been designated as the AMLO. The AMLO has the authority to act independently in carrying out his or her responsibilities and will be provided with access to sufficient resources to carry out his or her duties.

The AMLO has knowledge of the ML risks associated with the Company's operation and understands applicable federal regulations. The AMLO is responsible for effectively developing, implementing, overseeing, and managing the AML program within the Company. To this end, the AMLO's duties may include the following:

- Reporting to Senior Management about the effectiveness of this Policy;
- Maintaining records created in accordance with this Policy;
- Receiving internal disclosures and determining whether these should be reported to the appropriate governmental authorities;
- Training employees to ensure they are aware of the AML Policy;
- Serving as the internal point of contact for reports stemming from suspicious transactions or suspicious activities.

The AMLO is also responsible for monitoring changes in the law and federal regulatory scheme that could impact the Company's AML program. The AMLO will be responsible for apprising employees of such changes and ensuring that the Policy and employee training accurately reflect the current state of the law.

If any AML-related tasks are delegated in the business, the AMLO will remain responsible for supervising the employee to whom the task has been delegated.

c. Employees' Responsibilities

All employees will be trained to follow this AML Policy and to carry out the AML measures described herein. Employees must report to the AMLO any knowledge or suspicion of ML, whether by customers or other employees. Reports made to the AMLO will remain confidential. Employees are advised to remain vigilant and cognizant of the risks of ML within the Company, and to diligently fulfil their legal obligations to report suspicion of any such activity.

d. Review of the Policy

The Company will conduct an audit (either internal or external) of the AML Policy on an annual basis. The results of this audit will be reported to the AMLO. The AMLO will determine, based on the results of the audit, whether changes need to be made to the substance or implementation of the Policy.

7. AML Framework

a. Money Laundering in Practice

Money laundering is defined as the process of covering up or “laundering” illegally obtained money to wipe away traces of criminal activity and make it appear as if it were legitimately obtained. When criminal activity generates substantial income, the individual or group involved must find a way to channel the proceeds of the crime through the financial system without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. If undertaken successfully, money laundering allows criminals to maintain control over and enjoy their ill-gotten proceeds.

Money launderers seek to exploit the facilities of the world’s financial institutions and e-commerce platforms to benefit from the proceeds of their criminal activities. The increased integration of the world’s financial systems, the removal of barriers to the free movement of capital, and technological developments have enhanced the ease with which criminal money can be laundered, thereby complicating the tracing process.

There are two main forms of money laundering in the gambling sector:

- (1) Exchanging money, assets, goods, and property that were acquired criminally for money or assets that appear to be legitimate or “clean.” This is achieved by transferring or passing the funds through some form of legitimate business transaction or structure.
- (2) Using criminal proceeds to fund gambling as a leisure activity.

b. Overview of the Structure of the AML Program

This AML Policy is governed by AML laws and regulations as well as a “best practices” approach to AML. At the heart of these laws and practices is a risk-based approach to identify, assess, mitigate, and manage potential ML risks within the Company. ML risks may vary from one sector to another and from one business platform to another. Therefore, to ensure that the AML measures, policies, controls, and procedures are effective, the regulations oblige business in potentially high-risk sectors to implement measures on a risk-sensitive basis through the adoption of a risk-based AML policy. This requires the Company to (1) identify and assess the ML risks it is exposed to; and (2) adapt these measures, policies, controls, and procedures in a way that ensures that resources are applied where they are most needed.

A customer-specific risk assessment will be carried out so that the Company is able to identify potential risks of engaging in a business relationship with a particular customer. This assessment enables Jack’s House to develop a risk profile for the customer, categorize the ML risk posed by the customer, and implement AML measures and procedures that are commensurate to the risk posed by the customer.

The advent and popularity of virtual currency has resulted in increased scrutiny from law enforcement and regulators. As a result, regulatory restrictions and obligations are constantly evolving. Jack’s House is mindful of this dynamic regulatory environment and, accordingly, adopts a fluid approach to its AML Policy – allowing for flexibility to adapt and update the Policy as needed.

7.1 The AML Policy

a. Customer Registration and Know Your Customer (“KYC”) Protocol

The Company will take appropriate steps to obtain relevant identifying information from customers who are utilizing the platform.

To this end, each new customer must register by providing their name, address, date of birth, and email address. Instead of creating a password, they will log in using their email address, after which they will receive an email with a verification code to access their account. When an account is created, a verification link will be sent to the email account provided during the registration process. When the user clicks on the link, the account will be activated and officially created. Customers are permitted to register only one player account in their name.

For each new customer, registration will require acknowledgment and acceptance of the Company’s Terms & Conditions. The customer must also complete an age acknowledgement checkbox, verifying that he or she is over the age of eighteen. No underage customers will be permitted to play on the platform. Jack’s House is committed to preventing underage people from using its platform and will take all necessary steps to ensure they are not permitted to create an account.

b. Verifying Customer Identity

When depositing or withdrawing over €2,000 (XCG 4,000), whether in a single transaction or in several transactions that total €2,000, the Company will require customers to provide documentation to verify their identity. Verification can be obtained by requiring the customer to provide either of the following:

- (1) A government document that verifies either (a) the name and address; or (b) the name and date of birth of the customer; or
- (2) A government document which verifies the customer’s full name and a second supporting document which verifies their name, address, and/or date of birth.

The following sources may be accepted for verification of customers:

- Current passport
- Birth Certificate
- Current Photo Card Driver’s License
- Residence Permit issued by the Home Office
- Firearms Certificate or Shotgun License
- Tax Bill or Statement
- Utility Bill or Statement containing current address
- Bank or Credit Union Statement containing current address
- Confirmation of an Electoral Register
- Attorney Letter Confirming Recent House Purchase or Land Registry Confirmation of Address
- Rent Bill or Statement
- Lease
- House or Car Insurance Certificate containing current address

Each customer’s KYC information will be kept for five years from the end of the business relationship or the customer’s last visit to the platform.

i. Customer Geolocation

Customers who are in “geo-blocked” jurisdictions will not be permitted to access and engage with the platform.

ii. Sanctions Name Screening

The imposition of economic sanctions against foreign countries remains an important instrument for the international community in the enforcement of laws related to money laundering and fraud. Sanctions can encompass a wide variety of measures, which include limitations on official and diplomatic contacts or travel, and the imposition of legal measures to restrict or prohibit trade or other economic activity. The Company has an obligation to abide by these economic sanctions, to aid in the enforcement of these laws and to meet applicable regulatory requirements.

To this end, the Company will periodically review the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC) Specifically Designated Nationals and Blocked Persons List (the “Designated Persons List”). Customers’ names will be compared against the OFAC Designated Persons List at the time the customer’s ID is reviewed. If a customer’s name is listed on the Designated Persons list, he or she will not be permitted to create and/or maintain an account with the Company and the AMLO must be notified. This process is described in further detail below.

c. Customer Risk Assessment

The Company will carry out a Customer Risk Assessment with the objective to:

- Assess a customer’s ML risk;
- Determine the level of due diligence required that would be appropriate with the customers’ identified level of risk;
- Determine the frequency for ongoing monitoring and customer information updates;
- Ascertain the level of management review and approval required.

i. Extreme and High-Risk Customers

Extreme Risk

Customers with information that has been confirmed by law enforcement agencies to be part of or affiliated with organized crime groups or are a positive match to a sanctions list are to be rated as Extreme Risk. If the Company becomes aware of this information, the business relationship is to be terminated immediately based on extreme ML risk.

If a customer is identified and confirmed as a positive match for the OFAC Designated Persons List, the user account will not be created or terminated if already created, with the Company’s AMLO immediately informed. The AMLO will consult with legal counsel to determine all necessary reporting requirements.

High Risk

Any customer that engages in any of the following behaviors will be categorized as High Risk and subject to Extra Due Diligence (“EDD”) procedures:

- The customer’s one-month deposits exceed the equivalent of \$25,000 (XCG 50.000);
- The customer demonstrates unusual velocity in his or her activity. This means that the customer changes the volume or value of transactions in a manner that is inconsistent with expected behavior;
- The customer requests that their funds be sent to several different accounts;

- The customer engages in an unusual withdrawal pattern such as artificially splitting redemptions to remain “below the radar.” For example, splitting a payout of \$2,000 (XCG 4.000) into four payouts of \$500 (XCG 1.000) within a short period of time with the hope of avoiding a request for further identification;
- The customer makes a withdrawal of more than the equivalent of \$15,000 (XCG 30.000) in cryptocurrency in a 24-hour period.

Employees responsible for customer and transaction monitoring should seek guidance from the AMLO if they identify a pattern of behavior that is not listed above but is otherwise potentially suspicious. The AMLO, relying on applicable laws, regulations, and internal policies, will determine whether the identified behavior should be considered “High Risk.”

- When a customer is identified as “High Risk,” the AMLO must be notified on the AML Slack channel. The AMLO will be responsible for determining whether the High Risk Customer should be required to provide evidence of source of funds. If the AMLO determines that, given the particular characteristics of the High Risk customer, requiring evidence of source of funds is appropriate, the following procedures will be implemented until the High Risk Customer has submitted the requisite evidence of his or her source of funds: Put all monies owed to the customer into an account (or equivalent) from which no withdrawals can be made.
- Additional deposits can be made into the account provided that they are “locked” until verification occurs.
- Bets can be made from the account, provided that any winnings are “locked” until verification occurs.
- When the proof of source of funds is provided, the customer’s account will be unlocked and withdrawals may resume.
- If the customer cannot or will not provide proof of source of funds, the business relationship will be terminated. If there are monies to be repaid, the amount repaid will consist of the monies owed to the customer at the point that the customer was labeled as “High Risk,” and proof of source of funds was triggered, plus any deposits made at that point and thereafter. All monies will be returned to the originating account.

d. Customer Due Diligence

By adopting a risk-based approach, the Customer can determine the extent of due diligence required on a risk-sensitive basis. A risk-based approach also helps the Company to direct resources proportionately in accordance with the ML risk posed.

Customer Due Diligence (“CDD”) includes ongoing monitoring of business relationships and transactions (discussed below) to identify suspicious activity or patterns to be recorded and, if warranted, reported to the appropriate Governmental authorities.

e. Enhanced Due Diligence (“EDD”)

The Company must apply extra measures and controls to mitigate/manage the risk associated with High Risk customers. The Company must apply EDD to customers rated as High Risk, which require regularly reviewing customers transaction histories and customer trends to identify patterns that require further examination.

Additionally, in certain circumstances, High Risk customers subject to EDD will be required to provide evidence of source of funds before being permitted to make deposits or wagers. The AMLO will determine (1) whether the High Risk customer will be required to provide proof of his or her source of funds; and (2) the appropriate forms of documentation that may be provided as evidence of source of funds. As noted above, if the AMLO determines that the High-Risk Customer must submit proof of his or her source of funds, the High Risk Customer will not be permitted to make a withdrawal from his or her account until the customer

provides the requisite verification. Failure to provide the requisite proof of source of funds will result in the termination of the customer's account. The AMLO will assess whether it is appropriate to report the customer to appropriate authorities.

All relevant staff understand that they are strictly prohibited from informing a customer that their account activity has triggered a report to the authorities. Employees are trained to understand that they must not inform or warn a customer that their transactions have been reported, either internally or externally.

If an employee of Jack's House believes, through the process of conducting EDD, that a customer is engaged in suspicious activity, he or she must submit a report to the AMLO. The AMLO will consider the report in light of all relevant information to determine whether or not to (1) consult outside legal counsel; and/or (2) report the suspicious behavior to the appropriate regulatory authorities.

Customers not assessed as High Risk do not require EDD.

Timeline for Compliance and Non-Compliant Documents

If the customer cannot provide compliant documents within 30 days from the moment the XCG. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the XCG. 4,000 thresholds, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

7.2 Targeted Financial Sanctions

Jack's House is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities based on the legislation as mentioned in paragraph 2.1. Mechanisms are established to ensure compliance with Jack's House legal obligations. This includes, but is not limited to, the following:

- Jack's House shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- Jack's House shall perform ongoing sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered and confirmed, Jack's House must immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and must immediately file a report with the FIU. Once the true match is confirmed by the supervisory authority, Jack's House shall terminate services and keep the frozen assets until further instruction from the supervisory authority, or otherwise, in light of tipping off considerations, follow instructions from the supervisory authority.

7.3 Politically Exposed Persons (PEPs)

A PEP is an individual who is entrusted with a prominent public function, other than middle ranking or more junior officials, including but not limited to the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers,
- members of parliament or of similar legislative bodies,
- members of the governing bodies of political parties,
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- members of courts of auditors or of the boards of central banks,
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces,
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

CDD Measures Specific to PEPs

Jack's House implements appropriate risk management systems to identify whether a customer or beneficial owner is a PEP, or a relative or close associate of one. This includes, at first instance, conducting comprehensive screening against reliable databases and lists to determine the PEP status of new customers during the onboarding process.

No business relationship shall be established or continued with a PEP before obtaining senior management¹ approval to service the PEP. This applies to new customers, ongoing relationships, and any occasional transactions.

In addition, the Company takes reasonable measures to ascertain the source of wealth and source of funds of the PEP. This involves:

- Requesting a statement from the PEP regarding their Source of Wealth.
- Verifying the statement through independent and reliable sources. Public sources will be consulted first, and if insufficient, additional documentation may be requested from the customer.

Additionally, the Company shall conduct enhanced ongoing monitoring of the business relationship, including analysis of the PEP's spending patterns to ensure they align with their declared legal sources of funds and the information on file.

In accordance with the risk-based approach that the Company employs, measures are tailored to the risk of the PEP, where the following are taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

PEP status screening will be conducted regularly throughout the business relationship. If a player who was not identified as a PEP at onboarding later becomes one, the Company is required to implement the enhanced due diligence measures outlined above within a thirty-day window of this determination. Failure to implement the required measures for newly identified PEPs within the specified timeframe will result in the termination of the relationship with that customer.

7.2 Monitoring

The Company is required to appropriately monitor all of the business relationships it has with customers as part of its normal due diligence practices. The purpose of ongoing monitoring is the following:

- (1) Ensure that all customer information is accurate and current; and
- (2) Continuously monitor customer transaction activity for unusual behavior and potentially suspicious activity.

Customer information must be kept up to date. This includes information that is retained by the Company from the customer, including the following:

- Name

¹ Senior management refers to individuals responsible for day-to-day operations or their immediate subordinates. Approval may also be sought from the Compliance Department manager.

- Date of birth to confirm that the customer is over 18 years of age
- Email
- Name screening for OFAC sanctions

If an employee of Jack's House believes, through the process of conducting Periodic Monitoring, that a customer is engaged in suspicious activity, he or she must submit a report to the AMLO. The AMLO will consider the report in light of all relevant information to determine whether or not to (1) consult legal counsel; and/or (2) report the suspicious behavior to the appropriate regulatory authorities.

f. Ongoing Transaction Monitoring

As part of its due diligence practices, the Company will have adequate controls in place to regulatory monitor customer activities for red flags and triggers.

The Company will monitor customer activities for unusual/strange patterns of behavior and suspicious activities that must be further investigated. The Company will have procedures in place to raise unusual transaction activity to the AMLO and associated risk management team. All reviews and investigation actions must be documented.

The following factors should be considered during the review of unusual transactions:

- Account activity history;
- Age of the account
- Transactions preceding purchases;
- Average spend amount of the customer;
- Average customer activity time on the platform;
- Account dormancy period
- Login history;
- IP address;
- Speed of activity;
- Source of funds; and
- Previous alerts or warnings on the account.

If after considering the above factors, the employee believes that the customer is engaging in suspicious activity, the employee should submit a report to the AMLO. The AMLO will consider the report in light of all relevant information to determine whether or not to (1) consult outside legal counsel; (2) report the suspicious behavior to the appropriate regulatory authorities; or label the customer as High Risk and implement the appropriate protocol.

Customers will be advised that their transactional behavior is subject to review by the Company's risk management team, and that pursuant to this monitoring, the Company reserves the right to freeze or cancel the account based on identification of suspicious activity.

Measures To Be Taken if a Customer Transacts More Than \$15,000 (XCG 30.000) in 24 Hours

If a customer makes a purchase of the equivalent of \$15,000 (XCG 30.000) or more (singular or cumulative) in a 24-hour period, the Company will be required to take additional steps to verify the customer's identity and source of funds. The AMLO will be notified, and senior management will determine whether to maintain the business relationship with the customer. The incident, and any approval of an ongoing relationship with the customer must be documented.

8. Collusion and Cheating

Jack's House has systems to detect cheating, collusion, and illegal activity. If cheating and/or collusion is identified, the customer's account will be terminated and, if appropriate, the customer will be reported to the authorities. If an employee is implicated in any cheating, collusion, or other illegal activity, they will be suspended pending a full investigation.

9. Reporting of unusual transactions

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the AMLO upon identification, providing a brief description of the specific mitigating measures taken.

All employees who engage with customers or have access to customer information receive anti-money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviors that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an Internal Unusual Activity Report to the AMLO in accordance with the Reporting Procedure. This ensures that the employee's legal obligation to report is fulfilled. Please see Appendix III for the Report form.

Employees are required to report any unusual activity to the AMLO immediately, but no later than 24 hours after the transaction has been executed, using the Internal Unusual Activity Report form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) business days. During this time, the AMLO may request additional information from relevant departments.

If the AMLO concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within 48 hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than 48 hours after the transaction has been executed.

9.1 Recognition of unusual transactions

Staff will be trained to recognize unusual transactions based on customer profiles and specific indicators. Reporting procedures to the AMLO will be established.

In accordance with the NORUT, Jack's House Name is observing both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. All such transactions must be reported to the AMLO in a format approved by management. Additionally, any supporting documentation, such as copies of identification, cash-out slips, and other relevant records, must also be submitted as supplements.

The AMLO is tasked with maintaining an organized filing system for these records. If the Company fails to report internally identified transactions to the FIU, the rationale for this decision must be thoroughly documented and signed by the AMLO and/or management. In accordance with the FATF Recommendations, the Company and its employees pays

particular attention to all complex or unusually large transactions, as well as any unusual transaction patterns that lack a clear economic or legitimate purpose.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to XCG 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 - i. A cashless transaction in the amount of XCG 5,000.00 or more.
 - ii. Accepting or releasing a deposit in the amount of XCG 5,000.00 or more at the request of the customer;
 - iii. Sale to a customer of chips in the amount of XCG 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 - iv. A cash out in the amount of XCG 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as "objective indicators", while (d) is referred to as "subjective indicator". While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of XCG 5,000.00 resets per game day of the user.

9.2 Prohibition of disclosure

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

Company has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

10. AML/CFT/CFP Training Program

One of the most important controls over the detection and prevention of ML/FT/FP activities is for the Company to have employees who are knowledgeable in ML/FT/FP risks and who are well trained in the identification of unusual activities or transactions that appear to be suspicious. The effectiveness of AML training is therefore an important component to the overall success of the Company's AML/CFT/CFP Policy.

The Company will implement AML/CFT/CFP training that advises employees of this Policy. Employees are required to complete the AML/CFT/CFP training at the time of new-hire onboarding (prior to any customer interaction or fulfillment of any AML/CFT/CFP -related activities). Employees may also be required to engage in ongoing/periodic “refresher training” as needed.

Form of Delivery

Employees will be advised of the contents of this Policy at the time of hire and as part of new-hire onboarding. The AMLO will determine the appropriate medium through which any additional information with regard to this Policy should be communicated to new employees.

Records of training completion, including the date of the training, will be kept in each employee’s personnel file.

Frequency of Training

There will be two instances when AML training is to be conducted:

- (1) **New Employee Onboarding:** New hires are required to complete training at the time of onboarding.
- (2) **Ongoing Training:** The Company will hold annual training sessions to refresh employee familiarity with this Policy and all applicable regulations. The applicable federal regulations or to this Policy.

Training Content

The AML training material will cover the substance of this Policy which includes the following:

- (1) Background on AML/CFT/CFP concepts and requirements:
 - a. What is ML/FT/FP?
 - b. The manner in which the Company could be vulnerable to ML/FT/FP activities.
- (2) Governance role and oversight:
 - a. Roles and responsibilities of the Company’s AMLO and
 - b. Roles and responsibilities of the associated risk-management team.
- (3) Policies and Procedures:
 - a. Policies and procedures developed by the Company.
 - b. Roles and responsibilities of the Company’s employees in detecting and deterring ML, including reporting obligations
- (4) Risk Assessment and high-risk customer management:
 - a. Provide an overview of high-risk areas.
 - b. Provide an introduction to risk-based approach and risk assessments.

11. Record Keeping

Requirements

The Company will maintain records of the actions taken to adopt and implement the risk-based approach outlined in this Policy, which may include the following:

- A copy of the Company's most recent AML Policy;
- A list of jurisdictions in which the Company operates;
- Any audit reports or assessments dealing with AML issues;
- All reviews and investigations conducted as part of the Company's ongoing customer and/or transaction monitoring practices; and
- Correspondence between the AMLO/Compliance department with staff members relating to AML issues.

The records must be kept for a period of at least five years.

Customer verification and KYC material must be maintained in line with the Company's internal data protection process.

12. Audit

On an annual basis the Company will engage in an audit (either internal or external) to review the AML Policy. The review is intended to evaluate the Company's AML Policy and to provide an evaluation on the effectiveness and adequacy of the AML Policy and resources (employees and systems), considering the size, complexity, and offerings of the Company.

The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

13. Appointment of a Compliance Officer

A senior AMLO be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AMLO officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

13.1 Duties of the AMLO

The AMLO shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the Company's efforts against money laundering and financing of terrorism and financing of proliferation.

Appendix I: Country Risk List

Please note that the risk classification in following list of countries is subject to continuous review. Any changes in risk indicators will be reflected promptly to ensure the list remains current and accurate.

High-risk countries

include:

1. Afghanistan
2. Algeria
3. Angola
4. Bangladesh
5. Barbados
6. Belarus
7. Benin
8. Bosnia & Herzegovina
9. Bulgaria
10. Burkina Faso
11. Burundi
12. Cambodia
13. Cameroon
14. Central African Republic
15. Chad
16. China
17. Colombia
18. Cote d'Ivoire
19. Croatia
20. Cuba
21. Cyprus
22. Democratic Republic of the Congo
23. Egypt
24. Eritrea
25. Ethiopia
26. Guinea
27. Guinea-Bissau
28. Haiti
29. Hong Kong
30. India
31. Indonesia
32. Iran
33. Iraq
34. Jamaica
35. Kenya
36. Kyrgyzstan

37. Laos
38. Lebanon
39. Liberia
40. Libya
41. Mali
42. Moldova
43. Monaco
44. Mozambique
45. Myanmar (Burma)
46. Namibia
47. Nepal
48. Nicaragua
49. Niger
50. Nigeria
51. North Korea
52. Pakistan
53. Panama
54. Peru
55. Philippines
56. Russian Federation
57. Senegal
58. Somalia
59. South Africa
60. South Sudan
61. Sudan
62. Syria
63. Tanzania
64. Thailand
65. Togo
66. Trinidad and Tobago
67. Tunisia
68. Türkiye
69. Turkmenistan
70. Uganda
71. Ukraine
72. Ukraine (Crimea, Donetsk, Lugansk)
73. United Arab Emirates

74. United Kingdom
75. Vanuatu
76. Venezuela
77. Vietnam
78. Yemen
79. Zimbabwe

Low-risk countries

include:

1. Australia
2. Canada
3. Denmark
4. Estonia
5. Finland
6. Germany
7. Iceland
8. Ireland
9. Luxembourg
10. Netherlands
11. New Zealand
12. Norway
13. Singapore
14. Sweden
15. Switzerland
16. Uruguay

Excluded markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Curaçao
7. Czech Republic
8. Denmark
9. Estonia
10. France
11. Germany

12. Greece
13. Hungary
14. Israel
15. Italy
16. Latvia
17. Lithuania
18. Netherlands
19. Poland
20. Republic of
Ireland
21. Saba
22. Serbia
23. Sint Eustatius
24. Sint Maarten
25. Slovakia
26. Slovenia
27. Spain
28. Sweden
29. Switzerland
30. United Kingdom
31. United States of
America

CONFIDENTIAL

Appendix II: Business Affiliate and Supplier Due Diligence

Company information:

Registered name and legal form	
Registration number	
Date of incorporation	
Registered address	
Status	
Ultimate Beneficiary Owners (UBOs)	
Persons with significant control (directors, members of supervisory board)	
Company website (if applicable)	

The documents below must be duly certified (where applicable) and, if they are not in the English language, provided with legalized translation in a language understandable by the Company Name:

Document	Remarks
Certificate of Incumbency showing the Ultimate Beneficial Owner(s) and Director(s)	
Recent Excerpt from the Chamber of Commerce or equivalent	
Certified copy passport of UBO(s) and Director(s)	
Proof of address of the UBO(s) and Director(s) no older than 3 months ²	
Proof of Licensing	
AML Policy	

² For natural persons who live or reside outside of Curaçao, and who are not personally identified by the provider, the NOIS mandates that the identity is established by either (1) a photocopy of an identification document (e.g. passport, ID card, driver's license) accompanied by a certified copy or extract from the Civil Registry of the person's place of permanent residence, or (2) following the electronic receipt of an identity document of the individual, within 2 weeks we receive a certified copy of the document.

Appendix III: Internal Unusual Activity Report

Date of report:		
Client ID:		
Date of account registration:		
Account status (Active/Suspended/Blocked):		
Risk rating:		
Account balance:		
Client details:	Full name:	
	E-mail:	
	Phone number:	
	Brand registration:	
	Date of birth:	
	Nationality/Country of registration:	
	Address:	
	Due diligence documents held:	
Reason for reporting:		<i>< explain what activity / transaction gave rise to the report ></i>
Date of unusual activity/transaction:		
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		
Reporting employee:	Signature:	Date:
Upon completion, please forward the form to the Compliance Officer as soon as possible.		

AML_CFT_CFP_Policy-Jack'sHouse_BV

Final Audit Report

2025-06-25

Created:	2025-06-25
By:	Bryon Finies (bryon.finies@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAADCWrGBhumKcC-lkzKg6tfJgSBDKHoSzb

"AML_CFT_CFP_Policy-Jack'sHouse_BV" History



Document created by Bryon Finies (bryon.finies@hbmgroup.com)

2025-06-25 - 3:42:38 PM GMT



Document emailed to Annesol Melaria (annesol.melaria@hbmgroup.com) for signature

2025-06-25 - 3:42:44 PM GMT



Document e-signed by Annesol Melaria (annesol.melaria@hbmgroup.com)

Signature Date: 2025-06-25 - 8:07:19 PM GMT - Time Source: server



Agreement completed.

2025-06-25 - 8:07:19 PM GMT



Adobe Acrobat Sign