

KNOW YOUR CUSTOMER (KYC) POLICY
MIRTH B.V.
(Reg. No. – 163936)



Stanislav Andrieiev, the
MLRO & Compliance
Officer



**Jonathan Marshall Ruwel
Heymans** obo Kurason Trust
Curacao N.V., the Managing
Director

CONTENTS

1.	GENERAL PROVISIONS AND POLICY STATEMENT	4
2.	AUDIENCE.....	4
3.	DEFINITIONS AND ABBREVIATIONS	5
4.	CUSTOMER RISK ASSESSMENT.....	6
5.	CUSTOMER ACCEPTANCE POLICY	7
6.	CUSTOMER KYC.....	9
7.	AWARE POLICY	10
8.	RELIANCE ON THIRD PARTIES TO PERFORM KYC	10
9.	REPORTING OF SUSPICIONS AND RECORDING.....	11
12.	UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION.....	14
13.	CONTACT INFORMATION	14
14.	POLICY HISTORY	14

KEY INFORMATION

Approving Official(s):	Stanislav Andrieiev, the MLRO & Compliance Officer Jonathan Marshall Ruwel Heymans obo Kurason Trust Curacao N.V., the Managing Director
Responsible Office:	Stanislav Andrieiev, the MLRO & compliance officer
Effective Date:	22.05.2025
Next Review Date:	22.05.2026

1. GENERAL PROVISIONS AND POLICY STATEMENT

- 1.1.1. Our company commits to conducting business with high ethical standards, ensuring all financial transactions comply with laws and regulations. We require all Customers to provide accurate and complete identification details during registration.
- 1.1.2. Our Company has the right to verify Customers' identities using trustworthy and independent sources, ensuring that the identity information is accurate. If this information becomes outdated, the Company may update it accordingly.
- 1.1.3. Our Know Your Customer (KYC) Policy is crucial for maintaining the integrity and security of our operations in the online gambling sector. This policy describes our processes for verifying customer identities, ensuring regulatory compliance, and preventing fraud, including money laundering and terrorism financing.
- 1.1.4. The primary goal of this Policy is to protect our Company from legal and regulatory risks by thoroughly vetting all Customers. This process seeks to verify each Customer's identity and legitimacy, deter illicit use of our platform, and improve transparency and trust.
- 1.1.5. This policy applies to all Customers registering and participating in gaming activities on our Website. It covers procedures related to customer identification, verification, and continual monitoring of account activities.
- 1.1.6. This Policy will be implemented alongside our General AML Policy, General AML Guide, Privacy & Management of Personal Data Policy, and any other internal regulations issued periodically by our Company.
- 1.1.7. Our KYC policy, procedures, and internal controls are designed to comply with FATF, GCB regulations, and general AML rules. They will be regularly reviewed and updated to address regulatory and business changes.
- 1.1.8. Our Company develops and provides training programs for all personnel involved in transactions as listed in the NOIS and the NORUT, including guidelines on employee conduct and ongoing education to foster awareness of the Company's policies against money laundering and terrorist financing.
- 1.1.9. Our Company may engage third parties to carry out certain KYC procedures, ensuring confidentiality is maintained.
- 1.1.10. Employees must not reveal any suspicion of money laundering to the suspected person or any external party. If contact with the Customer poses challenges, employees should consult and follow the directives of the Responsible Person.

2. AUDIENCE

- 2.1. This policy affects and regulates:
 - 2.1.1. **Casino Management and Staff:** Senior management and operational staff are crucial in implementing and monitoring KYC policies, understanding requirements, ensuring compliance, and fostering a vigilant, ethical culture within the Company.
 - 2.1.2. **Compliance Officers:** These individuals develop, implement, and supervise our compliance program, ensuring adherence to laws and regulations, and often acting as the primary point of contact between the casino and regulatory bodies.
 - 2.1.3. **Technology and IT Teams:** Responsible for deploying and managing technological solutions that facilitate customer monitoring, due diligence, and reporting systems vital for AML and CTM compliance.
 - 2.1.4. **Customers:** While not directly involved in policy formulation, customers are pivotal as policies affect their interaction with the casino, ensuring their transactions are secure and legitimate, thereby enhancing trust.
 - 2.1.5. **Investors and Stakeholders:** They have an interest in KYC compliance as it can affect the casino's financial performance and reputation, impacting their investments directly.

- 2.1.6. **Financial Institutions:** Banks and financial partners require assurance that our Company adheres to strong KYC policies to maintain banking relationships and smooth financial operations.
- 2.1.7. **Legal Team:** Tasked with advising on regulatory demands and potential legal consequences of policy breaches, ensuring casino policies align with legal and international standards.
- 2.1.8. **Third-party Suppliers:** Entities that provide services and products to our Company.
- 2.2. These KYC standards and procedures ensure that staff at all levels actively prevent the Company's services from being used for money laundering and related activities, with goals including:
 - 2.2.1. Complying with Anti-Money Laundering Act and regulations of applicable jurisdictions.
 - 2.2.2. Requiring employees to prevent, detect, and report all potential instances of the Company or its facilities being used for illegal activities, such as money laundering and terrorist financing.
 - 2.2.3. Mandating relevant employees to participate in anti-money laundering training to understand responsibilities under FATF and stay updated on anti-money laundering developments.
 - 2.2.4. Protecting the Company and its staff from risks associated with legal, regulatory, and supervisory breaches.
 - 2.2.5. Safeguarding the Company's reputation against the risks of being implicated in money laundering and terrorist financing activities.
 - 2.2.6. The Company will ensure this Policy adheres to legal and regulatory requirements, conducting an annual independent KYC policy compliance audit. The results will inform appropriate recommendations for action. The Company will grant the necessary authority and resources for implementing a compliant AML regime continuously.

3. DEFINITIONS AND ABBREVIATIONS

- 3.1. AML – means Anti-Money Laundering.
- 3.2. CFT – means Combating the Financing of Terrorism.
KYC – means Know Your Client.
- 3.3. Company – means Mirth B.V., a legal entity validly registered and existing under the laws of Curacao, identification number: 163936, address: Schottegatweg Oost 10 Unit A1K 10 Unit 1-9, Bon Bini Business Center, Curacao.
- 3.4. CDD – means Customer Due Diligence.
- 3.5. GCB – means Gaming Control Board of Curacao.
- 3.6. POCA – means The Proceeds of Crime Act.
- 3.7. OFAC – means Office of Foreign Assets Control.
- 3.8. SDN – means Specially Designated Nationals and Blocked Persons list ("SDN List").
- 3.9. FATF – means Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
- 3.10. NAF – means Netherlands Antillean guilder, the currency of Curaçao.
- 3.11. NOIS – means National Ordinance on Identification when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2010, no. 40 as last amended by N.G. 2015, no. 69).
- 3.12. NORUT – means National Ordinance on the Reporting of Unusual Transactions (Lands- verordening Melding Ongebruikelijke Transacties, N.G. 2010, no. 41 as last amended by N.G. 2015, no. 68).
- 3.13. FIU – means The Financial Intelligence Unit Curacao.

- 3.14. PEP – means an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals: (i) 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, (ii) 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 armed forces; (iii) 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 previously: (i) family members of the individuals listed previously, including spouse, partner, children and their spouses or partners, and parents, (ii) known close associates of the individuals listed previously, 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.
- 3.15. Gambling or Gambling Game — means any online game posted on the Website that means playing a game of chance for a Prize. Game of chance includes (i) a game that involves both an element of chance and an element of skill, (ii) a game that involves an element of chance that can be eliminated by superlative skill, (iii) a game that is presented as involving an element of chance but does not include a sport.
- 3.16. Reporting Form – means the standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction.
- 3.17. Customer — means an individual, who uses the Website and/or familiarizes himself with the provisions of the Website, these Policy and the provisions of other documents, and intends to register on the Website to participate in Gambling (acquire a Player status).
- 3.18. Third Parties — means any individuals and/or legal entities other than the User and/or the Player, in particular, but not exclusively: family members, spouses, friends, partners, counterparties, creditors, service providers, agents, etc.
- 3.19. Website — means the official websites of the Company, on which Customer may play the Gambling Games.
- 3.20. In this Policy singular include the plural, and the plural include singular in cases of a need for interpretation.

POLICY IMPLEMENTATION

4. CUSTOMER RISK ASSESSMENT

- 4.1. Customer risks involve assessing the potential threats of money laundering and terrorism financing associated with a customer or customer category, which is essential for forming a comprehensive risk-based framework. Based on established criteria, the Company may evaluate whether a specific customer represents a heightened risk and how mitigating factors might influence that evaluation. The application of risk variables can either lessen or heighten the risk assessment.
- 4.2. Customer risk refers to the money laundering and terrorism financing risk arising from a relationship with an individual. Evaluating such risk typically involves examining the person's economic activities and/or source of wealth. Categories of customers potentially indicating higher risk include:
- 4.2.1. Customers with multiple income sources;
- 4.2.2. Customers with irregular income patterns;
- 4.2.3. Politically Exposed Persons (PEPs);
- 4.2.4. Individuals who spend large amounts (indicating money possibly derived from illegal activities);
- 4.3. Customers whose spending is inconsistent with their known source of wealth or income; 5.2.6. The misuse of third parties, where criminals employ others to gamble, disperse large cash sums, purchase chips, or cash out on behalf of someone else to evade CDD measures; 5.2.7. Customers employing multiple casino player accounts to

obscure their gambling activities.

- 4.4. Our Company establishes a threshold that signifies the upper limit of typical transactions. A customer with a single, regular income source poses a lower ML/TF risk compared to a customer with multiple income sources or irregular income streams.

5. CUSTOMER ACCEPTANCE POLICY

- 5.1. Customer acceptance Policy outlines the criteria for determining whether a Client can be accepted to open an account – or if the level of risk requires additional due diligence.
- 5.2. Know Your Customer (KYC) and Client Due Diligence (CDD) needs to be carried out prior to any business relationship or transaction or acceptance of customer transactions.
- 5.3. Prohibited customers include:
- 5.3.1. Persons who have refused to provide required information or documentation, fail to provide sufficient information, fail to provide information regarding their identity, or KYC cannot be conducted.
- 5.3.2. Persons who use alias or conceal their true names, or provide false information to conceal themselves.
- 5.3.3. Persons that triggers sanctions lists, as announced or provided by Money Laundering Officer (hereinafter referred to “MLRO”) and international organizations.
- 5.3.4. Persons suspected of using the Company as a money laundering channel or using the transactions to finance terrorism and proliferation of weapon of mass destruction financing.
- 5.3.5. Persons of illegal age (under the age of 18). No person under eighteen years of age (or the applicable majority age in that person’s jurisdiction) may be registered as a Player and any funds deposited or any money won by any such persons shall be forfeited to the Regulatory Authority.
- 5.3.6. PEPs (Politically exposed persons). A politically exposed person is an individual with a high-profile political role, or someone who has been entrusted with a prominent public function. These individuals present a higher risk of involvement in money laundering and/or terrorist financing because of the position they hold. The Financial Action Task Force (FATF) subsequently codified the term in its AML guidance, setting out the following 3 classifications of PEP:
- 5.3.7. Foreign PEP. Individuals entrusted with prominent public functions by a foreign country. This category of PEP may include: heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials’.
- 5.3.8. Domestic PEP. Individuals entrusted with prominent domestic public functions. This category includes ‘heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials’.
- 5.3.9. International PEP. The FATF sets out a third category of ‘International PEP’ – known as an individual entrusted with a prominent position by an international organization. This category of PEP covers ‘members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.
- 5.3.10. Players who reside in restricted countries according to the FATF recommendations shall pass Enhanced Due Diligence, that include the following:
- Albania
 - Barbados
 - Burkina Faso

- Cameroon
- Cayman Islands
- Croatia
- Democratic Republic of Congo
- Gibraltar
- Haiti
- Jamaica
- Jordan
- Mali
- Mozambique
- Nigeria
- Panama
- Philippines
- Senegal
- South Africa
- South Sudan
- Syria
- Tanzania
- Türkiye
- Uganda
- United Arab Emirates
- Vietnam
- Yemen
- Democratic People's Republic of Korea
- Iran
- Myanmar

- 5.4. Regular and continuous review of customer information needs to be conducted until a relationship with the client is terminated.
- 5.5. Transaction movements need to be tracked continuously until a relationship with the client is terminated.
- 5.6. Transaction reporting needs to be carried out in accordance with AML/CTPF laws. Once suspicious transactions that may constitute money laundering and terrorism financing are detected, AMLO needs to be notified immediately.
- 5.7. The client's risk levels on money laundering and terrorism financing need to be reviewed in accordance with the results of customer information review and customer transaction monitoring.

- 5.8. It is prohibited to use our services and play Gambling Games from Curacao, therefore, access to our Website from Curacao is prohibited.

6. CUSTOMER KYC

- 6.1. Before any opening of an Account there must be registration by the Client which involves the provision of accurate details to Company. It is the Client's responsibility to immediately provide the Company with updated information to any information / documentation provided at the initial Account opening stage. The Company may verify creditworthiness of a Client with third parties who previously provided any information on the Client.
- 6.2. The Company is entitled to conduct the Customer Due Diligence measures when:
- 6.2.1. Establishing business relations.
- 6.2.2. Carrying out occasional transactions on and/or above the monetary equivalent of EUR 2 200, or the equivalent of Naf. (National currency of Curacao) 4 000 in currency available on the Website (Enhanced due diligence shall be performed in this case).
- 6.2.3. There is a suspicion of money laundering or terrorist financing.
- 6.2.4. The Company has doubts about the veracity or adequacy of previously obtained Customer identification data.
- 6.3. Upon Registration, a Client must fill in all the information requested by the Company, and a Client is personally responsible for provision of complete and accurate information. When identifying the Customer, at a minimum the following information must be collected: full name; permanent residential address; date of birth; place of birth; nationality; identity number.
- 6.4. The Client has the responsibility to inform the Company of any updates or changes of his information. If the Company becomes aware that a person has provided false information We will immediately cancel that person's registration as a Player with the Company and close his Account.
- 6.5. The Company reserves the right to carry out verification procedures. In case the Company suspects that a Client provided false information, the Company are entitled to close and block Client's access to Account.
- 6.6. Verification procedures include:
- 6.6.1. Identification of a Client
- 6.6.2. In the framework of identification, the Company has a list of mandatory information that has to be collected from the Client. Mandatory information includes a valid email address, place of residence, and relevant payment information.
- 6.6.3. Also, the follow-up procedure includes the collection of the following documents:
- 6.6.4. identity document.
- 6.6.5. photo of both sides of the bank card from which the funds were deposited.
- 6.6.6. bank account statement from which the funds were deposited.
- 6.7. Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.
- 6.8. Additionally, the Company has to provide the procedure of email confirmation. After the representation of the documents listed above, the Company send email to confirm the email address. The email has an active clickable link that shall be opened by the Client to confirm the email.
- 6.9. Client's activity monitoring. The Company reserves the right to monitors transactions and closely monitors the

activity of the Clients. The purpose of the monitoring is checking if the Client use his/her account in the way that does not contradicts the usual Client's activity. What is more, Company monitor and verify the compliance of the Clients' transactions with their usual scope of activities. The Company compares new and previously collected data. Also, the Company monitor collected documents and data in general.

- 6.10. The Company shall, always, keep a secure online list of all registered Players. Any one individual can only register a single Account with the Company and multi-account practices are strictly prohibited.
- 6.11. The Company always provide repeat KYC when there are KYC triggers that include:
 - 6.11.1. New account information.
 - 6.11.2. Unusual account activity and transactions.
 - 6.11.3. Change in occupation.
 - 6.11.4. Change in player behavior.

7. AWARE POLICY

- 7.1. All staff must remain vigilant for signs that the Company's services could be exploited for money laundering or that they may encounter illegal or terrorist property during their work.
- 7.2. If a staff member becomes aware of a potential suspicion, they should collect relevant information available to them and assess whether there are reasonable grounds to suspect money laundering. Any additional details obtained, especially explanations for unusual transactions or instructions, should be documented in the Customer's file through normal procedures, but no references to suspicion of money laundering should be recorded in the file.
- 7.3. The obligation to gather information does not include conducting independent research or investigations beyond the sources readily accessible within the Company.
- 7.4. After reviewing the routinely available information, if the staff member is confident that there are no reasonable grounds for suspicion, no further action is needed. However, if reasonable grounds for suspicion exist, they must escalate the matter to the Responsible Person.
- 7.5. If a staff member personally observes or believes there are grounds to suspect money laundering, they must submit a suspicion report to the Responsible Person, using the format designated for that purpose. Reporting in this manner does not breach customer confidentiality.
- 7.6. Anyone who suspects money laundering must not discuss this suspicion with anyone outside the Company or with any other staff members unless they are directly involved in the matter.
- 7.7. No staff member should disclose any suspicion of money laundering to the individual suspected, regardless of whether they are a Customer, or to any outside party. If circumstances make contact difficult, the staff member must seek and follow the instructions of the Responsible Person.

8. RELIANCE ON THIRD PARTIES TO PERFORM KYC

- 8.1. Our Company may rely on third parties when performing elements of the KYC measures, provided that the criteria mentioned in this Policy are met. The third party should be subject to KYC and record-keeping requirements of the Company. The third party will have an existing business relationship with the Customer, which is independent from the relationship to be formed by the Customer with the relying institution (our Company). Where such reliance is permitted, the ultimate responsibilities for KYC measures remain with the Company relying on the third party. In this case, our Company should have an agreement with the third party being relied upon that copies of identification data or other relevant documentation relating to KYC requirements will be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. Our Company, however, remains responsible for the

carrying out of a Customer-based risk assessment, determining whether the customer is a PEP and conducting on-going monitoring.

9. REPORTING OF SUSPICIONS AND RECORDING

- 9.1. If the Company suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or terrorist organizations, it shall promptly report its suspicion to the FIU in accordance with art. 11 of the NORUT.
- 9.2. By virtue of article 11 of the NORUT, the Company shall report any unusual transaction or any intended unusual transaction to the FIU without delay. Unusual transactions shall be reported in compliance with the NORUT.
- 9.3. The following transactions or intended transactions are deemed unusual:
 - 9.3.1. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance
 - 9.3.2. Transactions which are in connection with money laundering or terrorism financing are reported to the police authorities or to the following department of justice.
- 9.4. We may file a voluntary FIU for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the FIU rule. It is our policy that all FIU will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the FIU.
- 9.5. We will retain copies of any FIU filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the forms. We will identify and maintain supporting documentation and make such information available to any appropriate law enforcement agencies, state regulators upon request.
- 9.6. The Company is recording each unusual transaction individually on a reporting Form. Individual reporting forms are numbered sequentially. Any Reporting Form that is voided shall be retained by the Company.
- 9.7. The Company is maintaining records, containing the information and documentation necessary to decide whether the objective of the KYC measures referred to in this policy was met, and to establish the background and purpose of transactions, for at least five years after the business relationship is ended, or after the date of the occasional transaction.
- 9.8. Each report about an unusual transaction will include at least the following information:
 - 9.8.1. The identity of the Customer.
 - 9.8.2. Nature and number of the identification document of the Customer.
 - 9.8.3. The nature, date, time and place of transaction.
 - 9.8.4. The amount, destination and origin of the funds, securities, precious metals, or other values involved in the transaction
 - 9.8.5. The circumstances that identified the transaction as unusual.
- 9.9. The Compliance Officer signs the reporting form if it is submitted manually.
- 9.10. The senior management (director, executive director, CEO, etc.) is entitled to sign the reporting form with the verbal consent of the Compliance Officer.
- 9.11. By virtue of article 11 of the NORUT, our Company reports unusual transaction or any intended unusual transaction to the FIU without delay. In order to do this, it should have clear procedures for internal and external reporting of unusual transactions in place. These should be communicated to its personnel. All unusual individual transactions or series of transactions, as mentioned in Policy Indicators Unusual Transactions, must

- be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.
- 9.12. The Company may use an electronic system approved by the FIU for this purpose, or submit a paper copy of the reporting form. Submission of paper forms shall not be done by fax for the purpose of data security. In either case, our Company will retain a copy of the reporting form for its own records, which are available to GCB agents upon request.
- 9.13. The Company providing information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year.
- 9.14. The Company making the following documents and information readily available:
- 9.14.1. Its written and approved policy and procedures on money laundering and terrorist financing prevention.
- 9.14.2. The name of each Compliance Officer responsible for the Company's overall money laundering and terrorist financing deterrence and detection procedures and her/his designated job description.
- 9.14.3. Records of reported unusual transactions
- 9.14.4. Records on unusual transactions which required closer investigations.
- 9.14.5. The completed source of funds declaration.
- 9.14.6. Schedule of the training provided to our personnel regarding money laundering and terrorist financing.
- 9.14.7. The assessment report on the Company's policies and procedures on money laundering and terrorist financing by the internal audit department or the Company's external auditor.
- 9.14.8. Required copies of identification documents.
- 9.15. The listing above is not limitative and does not exclude the Company from providing additional information and documentation if the GCB so requests.
- 9.16. In addition, the Company maintain a record in writing of its (i) policies, procedures and controls, (ii) any changes to those policies, procedures and controls, (iii) the steps the Company have taken to communicate the policies, procedures and controls or any changes to them, within the Company's business.
- 9.17. The Company may share information with financial institutions or governmental authorities regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Before we share information with financial institutions or governmental authorities, we will take reasonable steps to verify that the financial institutions or governmental authorities are entitled to receive that information according to the legislation.
- 9.18. We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information.
- 9.19. We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:
- 9.19.1. Identifying and, where appropriate, reporting on money laundering or terrorist activities;
- 9.19.2. Determining whether to establish or maintain an account, or to engage in a transaction; or
- 9.19.3. Assisting the financial institution or gambling operator in complying with performing such activities.
- 9.20. If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked asset and/or rejected transaction form with OFAC within 10 days.
- 9.21. Our Company is not only required to adhere to the stipulations of the National Ordinance for Identification of Services but are also required to detect and report either intended or completed unusual transactions. Our Company has adequate procedures in place that cover the following (i) the recognition of unusual transactions,

(ii) the documentation of unusual transactions, and (iii) the reporting of unusual transactions.

- 9.22. An unusual transaction is a transaction inconsistent with the Customer's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the Customer. The purpose of collecting Customer information is to provide the Company with documentation to assess the risk that may be associated with the Customer and to build a Customer profile to assess how the Customer is going to act within the framework of the business relationship. Based on the NORUT legislation, objective and subjective indicators have been established by means of which our Company should assess whether a Customer's transaction qualifies as an unusual transaction.
- 9.23. Our management provides our staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All these unusual transactions must be reported to the Compliance Officer in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements. The Compliance Officer must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the Company, the reasons therefore shall be adequately documented and signed off by the Compliance Officer and/or management.
- 9.24. In order to implement FAT recommendation, Our Company pays special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The following transactions or intended transactions are deemed unusual:
- 9.24.1. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- 9.24.2. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- 9.24.3. Transactions in the amount of equivalent of NAF. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to: A cashless transaction in the amount of equivalent of NAF. 5,000 or more. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the Customer. Accepting or releasing a deposit in the amount of equivalent of NAF. 5,000 or more at the request of the Customer.
- 9.25. A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAF. 5,000 or more and is considered per gaming day.
- 9.26. Our Company registered with the FIU and to obtain access to the goAML reporting portal after validation by the FIU. The FIU allows bulk reporting, therefore our account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

10. COOPERATION WITH AUTHORITIES

- 10.1. The Company shall cooperate fully with law enforcement and regulatory authorities, providing requested information within 5 business days unless otherwise specified.
- 10.2. The Compliance Officer shall serve as the primary point of contact for such inquiries.

11. NOTIFICATIONS

- 11.1. The Company has the right to notify Customers when it requests information from them to verify their identities, in accordance with applicable legislation.
- 11.2. The Company may also send other notifications to Customers, such as termination notices, account blocking notices, warnings, and similar communications.

- 11.3. Notices to Customers will be delivered using methods such as email, phone calls, internal account messages, or postal mail.

12. UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION

- 12.1. The Company is required to check for amendments on Sanctions Decrees and Regulations on a regular basis and update the KYC policies and – procedures accordingly to reflect such amendments. Such information contains lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in (in any case):
- 12.1.1. The Consolidated United Nations Security Council Sanctions List.
- 12.1.2. The Sanction Decree “Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s.” (N.G. 2015, no. 29).
- 12.1.3. The Ministerial Regulation “Libya” (N.G. 2015, 28).
- 12.1.4. The Sanction Decree “Islamic Republic Iran 2015” (N.G. 2015, 27).
- 12.1.5. The Sanction Decree “Democratic People’s Republic of Korea 2015” (N.G. 2015, 30).
- 12.1.6. The Ministerial Regulation “Yemen” (N.G. 2015, 65).
- 12.1.7. Guidance for Financial Institutions in Detecting Terrorist Financing.
- 12.1.8. The listing¹³ of the Office of Foreign Assets Control (OFAC).
- 12.1.9. The National Ordinance on Identification of Customers when Rendering Services (N.G. 2017, no. 92).
- 12.1.10. The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99).
- 12.1.11. 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.
- 12.1.12. (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73).
- 12.1.13. The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).
- 12.1.14. National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34).
- 12.1.15. 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 Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council.
- 12.1.16. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nation Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28).
- 12.1.17. Kingdom Sanction Act (N.G. 2016, no. 54).
- 12.1.18. National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2).
- 12.1.19. The National Ordinance on Identification of Customers when Rendering Services (N.G. 2017, no. 92).

13. CONTACT INFORMATION

- 13.1. For any questions regarding this policy, please contact: support@auro777.win or send a mail on the address: Schottegatweg Oost 10 Unit A1K 10 Unit 1-9, Bon Bini Business Center, Curaçao.

14. POLICY HISTORY

May 22, 2025	KYC policy update (Annual update)
--------------	-----------------------------------

December 02, 2024	KYC policy update (legal changes)
July 25, 2024	KYC policy update (legal changes)
March 14, 2024	KYC policy update update (Annual update)
November 22, 2023	KYC policy update (legal changes)
July 20, 2023	KYC policy update (legal changes)
May 24, 2023	Initial KYC policy