

CRYPTOCURRENCY POLICY
MIRTH B.V.
(Reg. No. – 163936)



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

CRYPTOCURRENCY POLICY

MIRTH B.V.

Reg. No. – 163936

Schottegatweg Oost 10 Unit A1K 10 Unit 1-9, Bon Bini Business Center, Curaçao

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: 21.05.2025

Next Review Date: 21.05.2026

CONTENTS

Introduction and Policy Statement

Audience

Definitions and abbreviations

Cryptocurrency payments

Withdrawals

Volatility & Conversion

Required information about the Customer

Refund Policy. Errors and Wrong Addresses.

Transaction limits.

Security

Law and regulation

Customer Risk Assessment

Client acceptance Policy

KYC, Due Diligence and other AML/CTF/CWP measures

Policy updates and procedures. Related Information

Contact Information

Policy History

1. Introduction and Policy Statement

- 1.1. This Cryptocurrency Policy (the "**Policy**") offers detailed guidance relating the use of our services (games) with payments (deposits) in Cryptocurrency that are made available to our Customers on or through the Website. Our Services is provided only by **MIRTH B.V.** (hereinafter - "**Company**", "We", "Us", "Our"), according to the legislative and regulatory requirements. The main purpose of this Policy is establishing of an effective system of processes and rules while using our service (games) with cryptocurrency payments (deposits).
- 1.2. Our Company involves Third Parties with the aim of providing processing of payments in favor of our Clients for the services enabling acceptance of Virtual Assets as a payment for our Services. To use Virtual Assets payment service, our Clients shall be registered on the Website as the Client. The execution of payment for services using Virtual Assets is possible exclusively upon passing the Know-Your-Customer (KYC) procedure and Anti-Money-Laundering (AML) checks, and successful registration on the Website.
- 1.3. Virtual Currency wallet service on the Customer's account enables the Customer to transfer its balances of certain supported virtual currencies (collectively, "**Virtual Currency Transactions**"). Our designated Third Parties will process Virtual Currency Transactions in accordance with the instructions they receive from our Company. Virtual Currency processing service enables the Customer to send payments for our services and make pay-outs to our Customers in Virtual Currency on the checkout of our Website.
- 1.4. By initiating Virtual Currency Transactions or by sending and receiving virtual currency, the Customer appoints our Company as its nominee custodian to manage the Account where it is appropriate in the sole opinion of the Company, and the Company may involve Third Parties with the aim to provide processing of payments in favor of our Clients.
- 1.5. The services are available only in connection with those virtual currencies that our Company supports which may change from time to time. The Customer will not use the Account or its virtual currency wallet to store, send, request, or receive virtual currencies in any form that our Company does not support.
- 1.6. The Customer agrees that the Customer will not receive interest or other earnings in the Account or virtual currency wallet from the use of the services and the Company has no responsibility or liability to the Customer for Virtual Currency Transactions conducted by the Customer or conducted by the Company in accordance with Customer's instructions.
- 1.7. Our Clients are acknowledge, understand, and agree that Transactions with Virtual Assets are irreversible. As soon as the Client has confirmed the Transaction, and hence paid for the services as supplied to it by the Company in any Virtual Asset, the Transaction is irreversible, with no further obligation or liability of the Company with respect to the completed Transaction. It remains the duty and obligation of the Client to ensure that its use of Virtual Assets on our Website is made in accordance with Applicable Laws, which specifically includes without limitation any guidelines which may be issued by any regulatory body with jurisdiction over the Client. The Company shall have no liability or responsibility to the End User under any circumstances.
- 1.8. We are not your broker, intermediary, agent or advisor and we have no fiduciary relationship or obligation to you in connection with any Transactions or other activities you undertake when

using the our Services. We do not provide investment or consulting advice of any kind and no communication or information that we provide to you is intended as, or should be construed as, advice of any kind.

- 1.9. The execution of the payment for the goods and/or services of the Company by the Client is available as follows: (i) by settlement of the exact amount for the goods in supported Virtual Assets or (ii) by deposit of any amount in supported Virtual Assets on the Client's account.
- 1.10. Our Company has implemented security measures designed to secure the Client's information from accidental loss and from unauthorized access, use, alteration, or disclosure. However, the Company cannot guarantee that unauthorized persons will never gain access to the Client information, and the Client acknowledges that it provides such information at its own risk, except as otherwise provided by Applicable Laws.
- 1.11. The Company will regularly review this Policy to align with legal and regulatory standards and will conduct an independent audit each year to ensure the compliance. The audit results will be evaluated, and suitable recommendations will be proposed. The Company shall allocate the necessary authority and resources for the continuous enforcement of a compliant framework.
- 1.12. Subject matter, including the scope and applicability. Our policies, procedures and internal controls are designed to ensure compliance with all applicable regulations, general payment rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.
- 1.13. Purpose. This Policy aims to establish and improve the legal framework and practices that our Company must adopt to prevent, detect, and report any suspicious cases. Its primary objective is to ensure that illicit crypto funds are not processed through our financial systems. Additionally, this Policy includes regulations and guidelines designed to prevent our Company and casino from being used as a channel for terrorism financing, thereby ensuring that funds are not directed to support terrorist and laundering activities.
- 1.14. This Cryptocurrency Policy outlines the rules, standards, and practices governing the acceptance, use, storage, and withdrawal of cryptocurrencies on our Website. The purpose of this policy is to ensure transparency, security, and compliance with applicable laws and regulations while providing a safe and efficient environment for Customers.
- 1.15. Our Company shall monitor this Policy with legal and regulatory requirements and conduct an annual independent compliance audit, the findings of which are to be considered and appropriate recommendations for action set out. The Company shall provide the necessary authority and resources for the ongoing implementation of a compliant payment regime.
- 1.16. The Company has the right to engage third parties for certain payment functions, provided confidentiality is maintained.

2. Audience

- 2.1. This policy outlines the effects and regulations concerning:
- 2.2. **Casino Management and Staff:** Senior management and operations personnel are actively engaged in applying and supervising this policy and procedures. Their responsibilities include understanding requirements, ensuring compliance, and fostering a culture of vigilance and ethical conduct within the Company.

- 2.3. **Compliance Officers:** Individuals tasked with developing, executing, and monitoring our compliance program. They ensure that our Company aligns with pertinent laws and regulations, often acting as the primary contact between our Company and regulatory bodies.
- 2.4. **Technology and IT Teams:** These teams are responsible for implementing and managing technological solutions that support transaction monitoring and reporting systems necessary for the compliance.
- 2.5. **Customers:** Although not directly involved in policy formation, customers are crucial as these policies influence their experience with the casino and our Company. The policies help ensure that customers' transactions are secure and legitimate, strengthening trust in the casino's operations and our Company.
- 2.6. **Investors and Stakeholders:** Investors and stakeholders have a vested interest in adherence to our policies, as compliance can influence the casino's financial performance and reputation, thereby directly impacting their investments.
- 2.7. **Financial Institutions:** Banks and financial partners, cryptocurrency processors that process transactions for our online casino require assurance that our Company adheres to stringent crypto policies. This adherence is essential for maintaining banking relationships and ensuring smooth financial operations.
- 2.8. **Legal Team:** Responsible for advising on regulatory needs and potential legal outcomes of policy violations. They work to align the casino's policies with the current legal landscape and international standards.
- 2.9. **Third-Party Suppliers:** Entities that provide services and products to our Company.

3. Definitions and abbreviations

- 3.1. 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 Cente, Curasao.
- 3.2. Cryptocurrency or Virtual Assets – means a type of digital asset that (i) is issued and transferred using distributed ledger or blockchain technology, (ii) is secured by cryptographic techniques, (iii) functions as a medium of exchange, a unit of account, or a store of value, (iv) is not issued or guaranteed by any central bank or government authority, and (v) may be accepted by our Company as a method of deposit or withdrawal subject to the terms of this Policy.
- 3.3. CDD – means Customer Due Diligence.
- 3.4. GCB – means Gaming Control Board of Curacao.
- 3.5. POCA – means The Proceeds of Crime Act.
- 3.6. OFAC – means Office of Foreign Assets Control.
- 3.7. SDN – means Specially Designated Nationals and Blocked Persons list ("SDN List").
- 3.8. 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.

- 3.9. NAF – means Netherlands Antillean guilder, the currency of Curaçao.
- 3.10. 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).
- 3.11. NORUT – means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2010, no. 41 as last amended by N.G. 2015, no. 68).
- 3.12. FIU – means The Financial Intelligence Unit Curacao.
- 3.13. 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.
- 3.14. 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.
- 3.15. Reporting Form – means the standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction.
- 3.16. Customer or Client — 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).
- 3.17. 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.
- 3.18. Website — means the official websites of the Company, on which Customer may play the Gambling Games.
- 3.19. In this Policy singular include the plural, and the plural include singular in cases of a need for interpretation.

4. Cryptocurrency payments

- 4.1. To use the cryptocurrency payments via Customer's Account on the Website, our Client shall:
 - 4.1.1. Be at fully legal capacity to enter into agreement with our Company (stipulated in Terms and Conditions) and use the Website and the services.
 - 4.1.2. Reside in a country where the Website and Services are legally accessible. The list of Restricted Territories is available on the Website and may be changed from time to time.
 - 4.1.3. Have the relevant knowledge to use Website and Services.
 - 4.1.4. Agree to comply with Terms on the Website.
 - 4.1.5. Pass the KYC and Due Diligence procedures.
- 4.2. Before the payment in cryptocurrency, our Company will ask, and the Customer is required to prove the information and documents including, but not limited to financial details, including source of wealth, source of income, registered and physical address, personal information relating to the family with the aim to identify a possible Peps, controlling persons, other related persons. The information that the Customer provides must be accurate and complete and the Customer shall inform the Company in writing within 10 business days of any changes to such information. Failure to provide the required information shall lead to refusal by the Company to provide payment in cryptocurrency. The Company may also obtain information about the Customer from third parties, such as credit bureaus, identity verification services, public registers, etc.
- 4.3. Our Company reserves the right to require from the Customer any additional information and documents related to KYC and AML checks at any time, which Customer is obliged to submit at the earliest opportunity. Failure to provide the required information shall lead to suspension or termination of providing the Services and to closing of the Customer's Account.
- 4.4. Once successfully passed the KYC and AML procedures with the Company, the Company will provide the Client the access to its Account through the Website. Our Customer should keep its personal username and password secret, secure, and make sure that they are not stored in a way that enables others to access them or impersonate the Customer. If Customer discloses its personal username and password to any person whom Customer authorizes to access its Account, Customer shall be also solely responsible and liable for any access, use, misuse, or disclosure of its personal username and password to its Account by such person.
- 4.5. Customer may have only one Account with the Company.
- 4.6. Customer shall immediately notify the Company by e-mail with remark "Urgent" or to its dedicated client manager in case of discovering or suspecting the following:
 - 4.6.1. The loss or disclosure to any unauthorized person of Customer's personal username and password;
 - 4.6.2. Any unauthorized access to Customer's Account;
 - 4.6.3. Any other criminal or fraudulent activity relating to Customer's Account;
 - 4.6.4. Any other breach of security relating to Customer's Account, whether physical or relating to computer or similar hardware or software.

- 4.7. When receiving such a notification from the Customer or determining that the security of Customer's personal username and password may have been breached, the access to the Customer's Account shall be suspended until measures have been taken to verify its identity.
- 4.8. Our Company and designated Third Party may refuse to process or cancel any pending Virtual Currency Transaction as required by law or any court or other authority to which the Company is subject in any jurisdiction. The Company further reserves the right to delay any Virtual Currency Transaction if the Company perceive a risk of fraud or illegal activity. Our Company also has the right to refuse to process or cancel any Virtual Currency Transaction due to technological issues with the blockchain software, its own software, or for other technological reasons.
- 4.9. To facilitate compliance with global industry standards for data retention, our Customers agree to permit us (but agree to not require us) to keep a record of all Transaction information for the lifetime of your Account as long as it is required to fulfil their intended purposes, or such other period as prescribed by Applicable Law. Please review our Privacy Policy for more information on how our Company collects and use data relating to the use and performance of our Website and the services.
- 4.10. Our Website may accept a limited number of widely used cryptocurrencies for deposits and withdrawals. Currently accepted currencies include:
 - 4.10.1. Bitcoin (BTC)
 - 4.10.2. Ethereum (ETH)
 - 4.10.3. Litecoin (LTC)
 - 4.10.4. Tether (USDT)
- 4.11. Our Company reserves the right to add, suspend, or remove supported cryptocurrencies at its discretion, without prior notice.
- 4.12. All deposits made in cryptocurrency must be confirmed on the relevant blockchain network before being credited to the Customers's Account. The number of confirmations required may vary by Cryptocurrency. Deposits must be made to the unique wallet address provided by the Website. Deposits sent to expired or incorrect addresses may not be recoverable.

5. Withdrawals

- 5.1. Withdrawals in cryptocurrency will only be processed to the same wallet address from which the deposit originated, unless otherwise approved through enhanced verification.
 - 5.1.1. Customers may be required to complete identity verification (KYC) and/or source of funds checks before withdrawals are processed.
 - 5.1.2. Transaction fees charged by the blockchain network will be deducted from the withdrawal amount.
 - 5.1.3. Processing times are subject to blockchain network conditions and internal risk reviews.
- 5.2. Our Company is entitled to limit the amount of withdrawals according to our Terms and Rules and/or AML policy.

6. Volatility & Conversion

- 6.1. Cryptocurrency deposits are credited in the equivalent value of the Website's base currency (e.g., USD or EUR) at the time of transaction confirmation.
- 6.2. The Website is not responsible for cryptocurrency price fluctuations. Customers bear the risk of volatility.
- 6.3. If applicable, the Website may use third-party payment processors or exchange services to convert cryptocurrency into fiat or stablecoins.

7. Required information about the Customer

- 7.1. We may require information from the Customer at any time for the purposes of complying with any Applicable Law, identity verification requirements, or in connection with the detection of money laundering, terrorist financing, fraud, or any other financial crime, or for any other valid reason. Clients agree to provide us with any such information we request and permit us to keep a record of the information for the lifetime of your Account as long as it is required to fulfil their intended purposes, or such other period as prescribed by Applicable Law.
- 7.2. Customer's access to the Account and the Transaction limits that apply to the use of our services may be altered as a result of information collected about the Customer on an ongoing basis. If there is a reasonable suspicion that any information provided by the Client is wrong, untruthful, outdated, or incomplete, our Company may send a notice to request corrections, remove relevant information, or do such other things that our Company consider necessary to ensure that the information provided by the Client is true and correct.
- 7.3. Our Customer should comply with any information request our Company sends. If our Client declines to provide the requested information, or otherwise does not comply in a timely manner, our Company reserves the right to suspend or terminate the access to Account, or to all or part of the services immediately, without notice.

8. Refund Policy. Errors and Wrong Addresses.

- 8.1. It is the nature of Bitcoin, Litecoin, and the other virtual currencies that our Company supports that all Virtual Currency Transactions are final with no method of refunding, charging back or other recourse for the sender of the virtual currency. As such the neither our Company nor the Customer are unable to cancel, reverse or provide refunds for any Virtual Currency Transaction made through the Services once it has been broadcast to the relevant Virtual Currency network.
- 8.2. If a Virtual Currency Transaction has not yet been confirmed on the Virtual Currency network, Virtual Currency associated with such transaction will be designated as pending and will not be included in the Company Virtual Currency wallet balance or be available to conduct Virtual Currency Transactions by the Client again. The Company cannot reverse or change any Virtual Currency Transaction marked as complete or pending.
- 8.3. The Client accepts and acknowledges that the Company is not liable or responsible for any errors or omissions whatsoever that are made in connection with any Virtual Currency Transaction initiated via the Services using the wrong details (i.e. destination address, tag, etc.). The Company strongly encourages the Customer to review its transaction details carefully before attempting to transfer a virtual currency.

9. Transaction limits.

- 9.1. The Customer's account may be subject to a limit on:

- 9.1.1. The amount or volume of Transactions our Client may undertake in connection with Account; and/or
- 9.1.2. The amount or value of Fiat Currency or Digital Assets our Client may transfer into or out of the Account, and/or
- 9.1.3. In each case in a given period (e.g. daily). Any applicable limits are shown in Client's Account.
- 9.2. Our Company reserves the right to change any Transaction limit that applies to the Client's Account at any time at our absolute discretion. It may also be possible for our Client requests a change in the limits. Any change will be made in our absolute discretion and will be subject to any further conditions that we deem necessary.

10. Security

- 10.1. Cryptocurrency funds are stored using a combination of hot and cold wallet infrastructure.
- 10.2. Multi-signature wallets and advanced security protocols are implemented to minimize risks of theft or loss.
- 10.3. Customers are responsible for securing their own wallets, private keys, and login credentials.

11. Law and regulation

- 11.1. Following the National Anti-Money Laundering Ordinance (1993), money laundering is a criminal offense in Curaçao. The following describes other major national regulations regarding money laundering and terrorist financing, among others:
 - 11.1.1. Criminal Code (Penal Code) (N.G. 2011, no. 48);
 - 11.1.2. National Ordinance for the Reporting of Unusual Transactions (N.G. 1996, No. 21), as last amended by N.G. 2009, No. 65 (N.G. 2010, No. 41) (NORUT);
 - 11.1.3. National Ordinance on the identification of customers in the provision of services (NG 1996, No. 23) as last amended by H. 2009, No. 66 (NG 2010, No. 40) (NOIS) together with all amendments thereto and all relevant national decrees, containing general measures, and decrees of the respective ministries concerning general operations;
 - 11.1.4. National Ordinance containing general measures to implement Articles 9, paragraph 2, and 9a, paragraph 2 of the National Ordinance on the identification of customers in the provision of services. (National Ordinance on General Penalties and Administrative Fines for Service Providers) (N.G. 2010, No. 70);
 - 11.1.5. National Sanctions Decree on "Al-Qaeda", "Taliban" in Afghanistan, Osama bin Laden, and terrorists to be listed locally (N.G. 2010, No. 93);
 - 11.1.6. National Decree on the obligation to report cross-border movements of money N.G. 2002, no. 74) together with all their amendments and all relevant national decrees containing general measures and ministerial decrees concerning general operations.
 - 11.1.7. International Standards of the Financial Action Task Force and the Caribbean Financial Action Task Force.

12. Customer Risk Assessment

- 12.1. 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.

- 12.2. 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:
 - 12.2.1. Customers with multiple income sources;
 - 12.2.2. Customers with irregular income patterns;
 - 12.2.3. Politically Exposed Persons (PEPs);
 - 12.2.4. Individuals who spend large amounts (indicating money possibly derived from illegal activities);
- 12.3. 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.
- 12.4. 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.

13. Client acceptance Policy

- 13.1. 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.
- 13.2. 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.
- 13.3. Prohibited customers include:
 - 13.3.1. 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.
 - 13.3.2. Persons who use alias or conceal their true names, or provide false information to conceal themselves.
 - 13.3.3. Persons that triggers sanctions lists, as announced or provided by Money Laundering Officer (hereinafter referred to “MLRO”) and international organizations.
 - 13.3.4. 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.
 - 13.3.5. 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.
 - 13.3.6. 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:

13.3.7. 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’.

13.3.8. 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’.

13.3.9. 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.

13.4. 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

- 13.5. Regular and continuous review of customer information needs to be conducted until a relationship with the client is terminated.
- 13.6. Transaction movements need to be tracked continuously until a relationship with the client is terminated.
- 13.7. 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.
- 13.8. 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.
- 13.9. It is prohibited to use our services and play Gambling Games from Curacao, therefore, access to our Website from Curacao is prohibited.
- 13.10. Players (Customers) residing in Curacao, the Netherlands (and any country forming part of the kingdom of the Netherlands), US, UN sanctioned countries and FATF blacklisted countries are not allowed to register an account.

14. KYC, Due Diligence and other AML/CTF/CWP measures

- 14.1. All Know Your Customer (KYC), Customer Due Diligence (CDD), Anti-Money laundering measures, Counter terrorism financing measures and Counter weapon proliferation measures and processes relating to cryptocurrency deposits and withdrawals shall be carried out in accordance with our Anti-money laundering and combating the financing of terrorism policy (AML/KYC) established in our Website.
- 14.2. The same standards for identification, verification, monitoring, and reporting that apply to fiat transactions are applied to cryptocurrency transactions.
- 14.3. Cryptocurrency activity is monitored for red flags, including but not limited to:
 - 14.3.1. Use of mixing services, tumblers, or privacy-enhancing tools;
 - 14.3.2. Structuring of transactions to avoid reporting thresholds;
 - 14.3.3. Transfers from/to wallets connected with high-risk or sanctioned jurisdictions;
 - 14.3.4. Activity inconsistent with the user's known profile.

- 14.4. All suspicious or unusual transactions are subject to internal review and, where necessary, reporting to the relevant Financial Intelligence Unit (FIU) or competent authority.
- 14.5. Accounts may be suspended or closed if users fail to comply with verification requests or are suspected of engaging in unlawful activity.

15. Policy updates and procedures. Related Information

- 15.1. It is the policy of this Company to monitor our compliance with legal and regulatory requirements and conduct an annual independent compliance audit, the findings of which are to be considered and appropriate recommendations for action set out. The Company's owner shall provide the necessary authority and resources for the ongoing implementation of a compliant Crypto payment regime.
- 15.2. The Company makes all necessary amendments to the Policy according to the changes in applicable legislation and FATF recommendations. Amendments to the Policy are done on an ongoing basis, but no later than three months after the entry into force of amendments to anti-money laundering and anti-terrorist financing legislation and/or identifying events that may impact on Policy.

16. Contact Information

- 16.1. 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.

17. Policy History

May 22, 2025, Cryptocurrency policy update (annual update)

December 02, 2024, Cryptocurrency policy update (legal changes)

July 25, 2024, Cryptocurrency policy update (legal changes)

March 14, 2024, Cryptocurrency policy update (annual update)

November 22, 2023, Cryptocurrency policy update (legal changes)

July 20, 2023, Cryptocurrency policy update (legal changes)

May 24, 2023, Initial Cryptocurrency policy