Banqua Sp z.o.o

Know Your Customer (KYC)

Disclaimer:

The document is prepared for the " Banqua Sp z.o.o" considering broader Know Your Customer (KYC) compliance requirements, and the information provided. This document should not be used for any other company or business whether in EU or any other jurisdiction. The responsibility to ensure policy confidentiality, periodic review, update, and approval of this document rests with the Board/Management of the company. The document should not be taken as an opinion on any AML/CFT or KYC related specific issue/ matter. All specific AML/CFT or KYC related issues/ matters faced by the company, shall be attended and looked after by the management and the MLRO of the company. AML/KYC subject matter expert may also be contacted by the company, for input or opinion.

Contents-

1	Objective	4
2	Scope and Confidentiality	4
3	Preparation and Approval	5
4	Target Audience	5
5	Policy Ownership	5
6	Know Your Customer (KYC)	5
7	Role of Board of Directors / Senior Management	9
8	Identification and Verification of Customers	10
9	Methods to Identify the Identity of Persons	12
10	Politically Exposed Persons (PEPs)	14
11	Transaction Thresholds and Monitoring	15
12	Record Keeping and Retention	16

1 Objective

Banqua Sp z.o.o, (referred to as “Company”) being registered in the register of Virtual Currencies as a cryptocurrency business is involved in wallet, custody, money transfer service, trading and investing in crypto currencies. The company does not deal in the fiat currencies. The company intends to do the crypto business in EU in a transparent manner and in compliance with applicable Know Your Customer (KYC) and anti-money laundering (AML) Act, laws, regulations and related requirements including EU AML Directive, to combat against the money laundering or financing of terrorism.

Virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities, therefore, to avoid these risks the Board and Management of the Banqua Sp z.o.o, ensures that appropriate KYC measures are implemented at all levels in the company.

Companies doing cryptocurrency business activities are subject to obligations under the AML Act if they provide the following services:

- exchange services between virtual currencies and FIATs (bureaux de change, exchanges);
- exchange services between virtual currencies (bureaux de change, exchanges);
- brokering services between virtual currencies and FIATs or between virtual currencies (as above);
- account maintenance services for virtual currencies (i.e. wallets).

The company aims to prohibit and avoid establishing business/customer relationships with sanctioned Individuals, proscribed persons, money launderers, terrorists, criminals and related groups or people. The company has implemented arrangements to identify and verify the customers before onboarding and establishing relationship with the customer. The company does not establish business relationships or provide services to the clients, customers or persons belonging to banned countries or jurisdictions including Iran, North Korea, Russia, Democratic Republic of Congo and other countries that are blacklisted or banned by the state or regulatory authorities of the jurisdiction or appearing in the sanction lists.

2 Scope and Confidentiality

This KYC policy is only applicable to the business operations and activities of the company, including wallet, custody, money transfer service, trading and investing in crypto currencies. This

KYC policy is a confidential document and shall not be replicated or used for any other company without consultation of relevant local AML/CFT regulatory experts or legal advisors.

3 Preparation and Approval

The preparation and implementation of KYC policy is the responsibility of Board/Management/Owner of the Banqua Sp z.o.o. The policy needs to be reviewed periodically to make necessary changes prescribed by regulators, and should be approved by the Board of Directors and Management of the company.

4 Target Audience

This KYC document is prepared for the management and employees of the Banqua Sp z.o.o who are expected to be vigilant in performing their day-to-day cryptocurrency business activities and operations. All employees of the company including account opening staff are required to ensure that all the customers or persons are identified, screened and verified before doing any business activity with them.

5 Policy Ownership

This KYC policy is owned by the Board/ Management of the Banqua Sp z.o.o. Account opening team and Money Laundering Reporting Officer (MLRO) of the company shall periodically review, and update (if necessary) this policy document. All the amendments and updations in the policy shall be approved by the Board and Senior Management of the company.

6 Know Your Customer (KYC)

Know Your Customer (KYC) is part of the CDD measures, which enables the organization to know the credentials, and background of the prospective customer. Organizations such as financial institutions are required to perform the KYC process before onboarding the customer and update the KYC later on different stages, such as during the process of periodic compliance reviews or investigations.

The KYC process protects an organization from being used for money laundering or terrorist financing activities, which may be performed by the customer, after getting onboarded by the organization, such as a financial institution. KYC enables the organization to avoid the risk of onboarding the criminals such as money launderers or persons associated with criminals in any manner. Onboarding the criminals causes the entity to face reputational losses, and imposition of

penalties from the regulator. KYC process is a mandatory process that is followed at the time when the customer contacts the organization either physically or through online portals, for opening an account, or provision of any services.

In the broader sense, the KYC process includes the following:

a) Client's identification using initial documents, provided by the customer.

b) Understanding the objective and purpose of opening the account or establishing the relationship.

Being in the cryptocurrency business, the Management of Banqua Sp z.o.o gives utmost importance, to prevent the risk of being used as a channel directly or indirectly for the money laundering or terrorist financing (ML/TF) purposes.

KYC requirements for clients require ID with names, photo, date of birth and proof of address. Senders and receivers of the funds are required to identify themselves with ID and proof of address.

Before opening the account, establishing business relationship and selling the services to the persons/ customers, the company obtains/checks the following:

- the account details including name, date of birth, photo, unique user ID, password,
- personal information including full name, residential address,
- Source of income / funds
-
- payment details/ information.

Account opening team/employees are responsible for ensuring that before providing services, the appropriate know your customer (KYC) process is applied, including identification, screening and verification of the clients/customer and his/her information provided at the time of opening account. Names of the customers are screened in the negative lists such as OFAC lists and other relevant prescribed negative lists/ databases for the black listed/ criminals and entities. Worldcheck screening shall be performed as part of the KYC process.

The screening of customers and related parties will be against the following (but not limited to) sanctions lists:

- OFAC Specially Designated Nationals (“SDN”) list
- OFAC non-SDN lists

- European Union (“EU”) sanctions lists
- United Nations (“UN”) sanctions lists
- UK Her Majesty’s Treasury (“HMT”) sanctions list

Additionally, Banqua Sp z.o.o will re-screen all customers when any of the aforementioned lists change, no later than three (3) business days following the lists changing.

Rescreening shall also be performed whenever customers updates their KYC information and in cases where the customers are suspected or found involved in any criminal activities, such as during performance of negative media search based on any information received regarding the customer, the information received from media news, information received from the regulatory body or announced by the state which raises doubts about the current customer of the company.

The account opening team, MLRO and third-party service provider shall periodically check the relevant websites and announcements of the organizations that provide screening lists such as OFAC, for the latest screening lists. The latest version of the lists shall be used to perform the screening. The Management and MLRO shall ensure that any positive match against, sanctions, PEP and adverse media list shall be notified to the Circle via email in circle AML Referral Email within 24 hours.

As part of the ongoing monitoring of the business relationships with customers, it must be ensured that the information of the client is kept up to date. The Banqua Sp z.o.o shall periodically review the information and transactions of the customers to assess the change in the risk profile of the customers. In case of change in the risk profile or transaction pattern of the customer, the information shall be asked from the respective customer regarding the source of income and in case of companies or businesses, the updated details of the principal business activities shall be asked. The information to be asked may relate to the nature of the customers/clients’ occupation.

This is necessary to ensure that the company maintains the updated information of its customers and clients. The updated information received form the customers/clients shall be identified and verified.

- Banqua

It shall be the responsibility of the MLRO and account opening team, to keep track of the sanction lists and other sources from where the prohibited countries, proscribed persons/customers or organizations can be identified. In case of third-party KYC arrangements, the MLRO and management of the company must ensure that the third-party service provider provide required KYC services to the Banqua Sp z.o.o.

Banqua Sp z.o.o shall abide by the following policy statements, as it relates to compliance with sanctions obligations:

- It shall not carry out any activities which includes making any funds or other assets, economic resources or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit of designated persons or entities; or behaving in a certain way contrary to applicable financial sanctions.
- It shall ensure that this Sanctions Policy and any other written policies and procedures concerning sanctions compliance remain adequate and effective, and therefore such policies shall be reviewed by the company's management or MLRO on at least an annual basis and re-approved and re-issued by the board of directors, at least annually,
- It shall ensure there is adequate and ongoing training of key staff on sanctions compliance as further set out in this Sanctions Policy.

List of Prohibited Jurisdictions:

The Board of Directors and Management of Banqua Sp z.o.o shall ensure that customers belonging to following countries are not onboarded or entertained:

- Afghanistan
- Belarus
- Central African Republic (the)
- Congo (the Democratic Republic of the)
- Cuba
- Guinea-Bissau
- Iran (Islamic Republic of)
- Iraq
- Korea (the Democratic People's Republic of)
- Libya
- Mali
- Myanmar
- Russia

- Somalia
- South Sudan
- Sudan (the)
- Syrian Arab Republic
- Ukraine
- Venezuela (Bolivarian Republic of)
- Yemen

Further, Banqua Sp z.o.o prohibits onboarding of customers in the following U.S. states:

- Alaska
- Hawaii
- Minnesota
- New York

To block the IP range and restrict the access to the app of Banqua Sp z.o.o the SHIELD software is used. Our platform is a mobile App, and it is not downloaded in stores (apple store and google store) in countries included in blacklists and countries that prohibit crypto). This restrict the user from prohibited jurisdictions. If, on the other hand, the app's activities are registered with an IP address in the prohibited jurisdiction, the user is disabled in the use of the app. Users will only be able to utilize the app if the IP is from an authorized jurisdiction.

7 Role of Board of Directors / Senior Management

The primary responsibility to develop and implement the strong KYC processes and controls is of the Board of Directors of the Banqua Sp z.o.o. The Board of Directors and Senior Management of the Banqua Sp z.o.o are responsible to:

- Ensure that Compliance Program is developed, including allied policies;
- Ensure that KYC policy is developed, reviewed and approved by the Board and Management;
- Ensure that KYC policy is disseminated to all the relevant employees of the company, to ensure its compliance;
- Ensure that third party service providers to perform KYC, are reputable and possess expertise in performing the KYC measures as per applicable laws and regulations;

- Ensure that third party service provider understand the requirements of confidentiality and has implemented appropriate internal controls, to avoid confidentiality issues;
- Ensure that third party service provider provide the KYC information of the customers or other persons, to the company;
- Ensure that KYC performed by the third-party service provider is checked and reviewed before opening account or onboarding customers;
- Ensure that obligation of compliance under relevant sanctions requirements are identified and complied with and no business activity or relationship is established with those appearing in the sanction list;
- Ensure that AML processes and controls are designed and implemented at all levels, to identify, verify and screen the customers of the company before establishing business relationship with them;
- Ensure that company does not open accounts, trade cryptocurrency transactions or performs any other business activity by way of any means, with criminals including money launderers, terrorists, tax evaders, proscribed persons, banned entities, defaulters, persons appearing in negative lists such as OFAC.
- Periodically review, discuss and resolve the KYC and AML issues, being identified by either MLRO or other employee, as per applicable AML/KYC regulatory requirements;
- Issue appropriate instructions and guidelines to the management including MLRO, in light pf applicable AML laws and regulations, to ensure that criminals including money launderers and terrorists are not entertained and ML/TF risks are managed on timely manner;
- Ensure that appropriate disciplinary actions are initiated in case of violation of AML regulatory and policy requirements;
- Ensure arrangements of periodic KYC training for the employees of the company, to ensure that they understand and remain updated with the applicable AML/KYC regulatory requirements.

8 Identification and Verification of Customers

The Banqua Sp z.o.o shall ensure that all the customers or persons with whom the company intends to do business or trade, are identified and verified. The company has entered into third party arrangements to perform the KYC on behalf of the company. It shall be ensured that third party service providers is a reputable firm or entity and possess AML/ KYC expertise. The KYC information of the customers or persons shall be obtained from the third-party service provider

and reviewed before opening account or onboarding customers. The KYC information shall be maintained by the company and only authorized person shall have access to the customer and KYC information.

Source of income/ funds shall be identified before onboarding and performing any business transaction with the customers. Source of income/funds should be genuine and from the legitimate source.

No account shall be opened or customer onboarded, in case of any fake identity document, inappropriate or fake source of income, source of income from any illegal business activity or from banned jurisdiction or country.

As a method of documentary verification, we include the following as part of the document scan, we confirm the following:

1. Automatic check ensures:

- ID document matches the official template
- MRZ, barcode, all related checksums
- Cross-check data from visual and MRZ zone
- Whether personal number exists
- Country/document-specific rules- Eg. doc number in France is 2 numbers 2 letters 5 numbers

2. If check needs to be reviewed manually we also check:

- Original document (real document, not a copy, printed out, screenshot etc)
- Security features and specific check eg. related to portrait (colours, other indicators)

The notice of the Customer Identification Programme shall be provided to the customer including terms of conditions will be presented both on the stowed, and within the app where the customer will be required to accept the terms and conditions.

CDD and KYC shall also be performed in case of:

a. Large number or value or transactions;

b. Large virtual currency (VC) transactions
c. Cryptocurrency transactions
d. Funds transfer by means other than an electronic funds transfer (EFT)
e. Foreign currency exchange transactions of over prescribed limit;
f. Exchanging VC in an amount equivalent to $1,000 or more
g. Remitting funds in the amount of $1,000 or more to a beneficiary, by means other than an EFT etc.

Triggers for KYC Performance:

Customers must be subjected to KYC in all of the following situations:

- Customer is withdrawing funds (both fiat and crypto) from its account
- Customer is an individual whose account is “open loop”, i.e., the wallet can hold USD Coin (“USDC”) and have on-chain access. This includes all “closed loop” customers wishing to withdraw funds
- Customer is an individual whose account is “closed loop”, and has reached either

of the following thresholds:

  - Customer has deposited the equivalent of $10,000 over the life of the account
  - Customer has a cumulative balance of the equivalent of $2,000 available during the course of a single calendar day. For example: if a wallet has a value of $1,500, and the customer spends $1,000 and subsequently reloads $600 before the end of the day, this wallet would have a cumulative daily balance of $2,100 and therefore be subject to KYC.

KYC is required prior to the account being opened. In the case of “closed loop” customers reaching thresholds, KYC is required prior to the customer being granted access to the funds that caused the account to reach the threshold.

BanquaBanqua.

9 Methods to Identify the Identity of Persons

The Banqua Sp z.o.o shall ensure that below mentioned minimum information is obtained and used for the identification and verification of the customers, persons:

For Individual users/ customers the Identification information shall be obtained and verified. The identification ID documents shall be collected and checked before opening the account.

The following information shall be taken from the individual customers before opening account:

- Full legal name
- Date of birth
- Residential address (must be a street address, not a Post Office (“PO”) box. If the individual does not have such an address, an Army Post Office (“APO”) or Fleet Post Office (“FPO”) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer's physical location is acceptable)
- Identification number (for U.S. customers, this is a Social Security Number (“SSN”) (or evidence of an application for one). For non-U.S. customer, this is one or more of the following: a taxpayer identification number; a passport number and country of issuance; an alien identification card number; or a number and country of issuance of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard)

National identification card and number, Passport, Driving License. The document must:

- be authentic, valid and current;
- be issued by a federal, provincial or territorial government;
- indicate the person's name;
- include a photo of the person;
- include a unique identifying number; and
- match the name and appearance of the person being identified.

It shall be ensured that the following information is recorded in the company’s records:

- the person's name;
- the date on which identity of the customer is verified;
- the type of document used (for example, driver's license, passport, etc.);
- the unique identifying number of the document used;
- the jurisdiction and country of issue of the document; and
- the expiry date of the document, if available (if this information appears on the document or card, you must record it)
- source of income/funds with evidence of proof.

No account shall be opened or transaction shall be made with such person, who failed to provide the correct identification and other KYC information.

As part of KYC process World check screening and screening from other negative lists shall be performed.

10 Politically Exposed Persons (PEPs)

The Banqua Sp z.o.o has the obligations to identify and verify the politically exposed persons (PEPs). Enhanced due diligence (EDD) shall be performed for the PEP and other high risk customers. Other high-risk customer includes persons belonging to high-risk jurisdictions etc. It shall be ensured by the MLRO and management of the Banqua Sp z.o.o, that third party KYC service provider performs the EDD measures in relation to the high-risk customers before onboarding or entering into a business relationship.

PEP metrics are managed by checkin.com with their metrics in the KYC process for screening each person. **The processes will be aligned with the firm's policy and decision making is** still held by the firm

The company shall create a risk profile of each customer based on the identification information and source of income/ funds provided by the customers at the time of onboarding or establishing business relationship. In case of transactions which appear inconsistent with the source of income and risk profile of the particular customer, the management of Banqua Sp z.o.o shall perform investigation to ensure whether the KYC profile of the customer needs to be updated. On the basis of investigations and proof of source of income/funds the KYC profile of the particular customer shall be updated in the records of the Banqua Sp z.o.o.

Enhanced Due Diligence Process (EDD):

An EDD is performed for high risk customers (as defined in Section 11 of our AML Policy) , and/or when a user exceeds the USDC 5,000.00 threshold in Fiat deposits or withdrawals. This is performed as additional check to better understand the background, purpose and the relationship of customer with Banqua Sp z.o.o. Customer is contacted by a representative of Banqua Sp z.o.o, to perform EDD where source of funds, proof of residence and other information is identified and verified, mentioned as follows:

1. Source of funds

To clearly indicate the source of funds and submit proof in support of their selected or provided statement which are:

-Bank statement where your income is clearly stated (salary)

-Employment contracts,

-Investment contracts/declarations,

-Balance of funds in current accounts and savings.

2. Proof of residence

Choose one of the following options:

-Utility bill (except mobile phone),

-Of electricity,

-Bank statement,

-Tax return/municipal tax.

If the EDD check is initiated the deposit will be suspended during the check, but no more than 5 days from the first day of contact with customer.

In case the customer does not pass the EDD process, the deposits shall not be accepted and all pending deposits will be declined and funds will be returned to original (origin) bank account.

Users who do not pass EDD control will be asked to empty their wallets completely up to zero balance and their user account will be disabled.

11 Transaction Thresholds and Monitoring

Management and the MLRO of the Banqua Sp z.o.o, shall ensure that the clients, customers, or persons with whom the company does cryptocurrency business are assessed from the risks point of view. MLRO shall ensure that risk profile of the customers, clients or persons, are created based on the KYC being performed before onboarding and establishing business relationship. Source of income should be legitimate and based on it, the risk profile shall be developed for each customer, client or person. Based on the risk profile, the transaction thresholds shall be created as a tool to monitor the activities of the clients, customers or persons with whom the company deals, invests or trade with.

MLRO shall ensure that transactions and activities of all the clients, customers or persons with whom Banqua Sp z.o.o has established business relationships, are regularly monitored considering the relevant risk profile and transaction threshold.

Any breach of the threshold or mismatch of risk profile shall be appropriately investigated and concluded by the MLRO and the management of the Banqua Sp z.o.o.

The company shall record all the transactions and shall separately identify the transactions, whose value exceeds threshold limits prescribed under applicable AML Act and regulations. MLRO is required to regularly check the prescribed limit under the current AML Act and regulations and report to relevant authority, (if required).

For transaction monitoring metrics, we will be provided by scorechain.com. The processes will be aligned with the firm's policy and decision making is still held by the firm

MLRO shall ensure that only those customers who pass the KYC due diligence process (as per KYC policy) may use account in the app. In case the suspicious transactions or activities are noticed over 5k USD then investigation shall be performed for those accounts and customers. Transactions shall be prevented to/from sanctions blockchain addresses, using Scorechain.com as the vendor used to control blockchain transactions. MLRO and AML service provider shall take control measures such as using sanction wallet screening tools to ensure that transactions are prevented from happening. Transactions are monitored by the MLRO on periodic basis to identify any suspicious activities or transactions in the accounts of the customers. Transaction monitoring may also be initiated based on the alert generated or reported by the service provider.

12 Record Keeping and Retention

a. Banqua

Banqua Sp z.o.o shall retain the following information about customers onboarded on for a minimum of seven (7) years following the date the account is closed:

- All identifying information received
- Descriptions of any steps taken to verify customers
- Any additional due diligence information collected

Additionally, Banqua Sp z.o.o shall retain:

- Copies of all ID documentation obtained from the customer for a minimum of seven years following the date the verification is performed

- Records of all sanctions, PEP and negative news screening performed, including any dispositions of alerts, for a minimum of seven years from the date the screening was performed

If customers request that their data be erased, for example under the EU General Data Protection Regulation, any such erasure must be conducted after the time periods stated above lapse.