

Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy

and

Know Your Customer (KYC) Policy

BMCP GmbH (“**BMCP**”) is a financial service institution according to § 2 Abs. 2 Nr. 3 & Nr. 5 WpIG (*Wertpapierinstitutsgesetz*), regulated by the German Financial Market Authority (*BaFin*). Thus, BMCP is authorized to provide regulated financial brokerage services using Blockchain technology. Our KYC process is in line with European financial market regulations.

Therefore, BMCP has put in place an Anti-Money Laundering / Counter-Terrorist Financing Policy and a Know Your Customer Policy (collectively, the “**AML Policies**”). The Policies are revisited periodically and amended from time to time based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing. All senior management and employees of the BMCP are required to acknowledge and be familiar with the Policies.

The Policies are designed to lay down a framework to:

- a) prevent BMCP from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities;
- b) enable BMCP to know/understand its customers, clientele, contributors, business associates, and other contacts with which BMCP has any financial dealings with (collectively, “**Dealing Entities**”) and their financial background and source of funds better, which in turn would help it to manage its risks prudently;
- c) put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, procedures and regulatory guidelines; and
- d) equip employees of BMCP with the necessary training and measures to deal with matters concerning KYC/AML procedures and reporting obligations.

THE POLICIES

RISK-BASED APPROACH

BMCP shall adopt and maintain a Risk-Based Approach (“**RBA**”) towards assessing and containing the money laundering and terrorist financing risks to BMCP arising any transactions it has with Dealing Entities. The guidelines are as follows:

- a) Before entering into any transaction or proposed transaction, necessary checks shall be conducted in line with the RBA so as to ensure that the identity of the Dealing Entities or persons associated with the entities does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations.

- b) For the purpose of risk categorization of Dealing Entities, the relevant information shall be obtained from the Dealing Entities at or before the time of entering into the transaction or commencement of business relationship.
- c) The risk categorization process for different types of Dealing Entities may take into account the background of the Dealing Entities, nature of business activity, country of origin, sources of funds, mode of payments, volume of turnover, financial background.
- d) The outcome of the risk categorization process shall be decided based on the relevant information provided by the Dealing Entities at the time of commencement of business relationship.
- e) Enhanced due diligence would be required for higher risk Dealing Entities, especially those for whom the sources of funds are not clear, or for transactions of higher value and frequency, which shall be determined by BMCP at its sole and absolute discretion.
- f) BMCP must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the Dealing Entities in compliance with the relevant legislations in place.
- g) If BMCP deems necessary, BMCP may appoint a Third-Party KYC/AML specialist screening firm to ensure compliance with prevailing regulations and BMCP policies. BMCP must be satisfied that such third party is adequately regulated, supervised or monitored, and has measures in place for compliance with Dealing Entities due diligence and record-keeping requirements in line with the requirements and obligations under the applicable regulations, and that the third party is not based in a country or jurisdiction assessed as high-risk.

1. DURING THE INVESTOR WHITELISTING

- 1.1 Establishing and maintaining risk-based due diligence, identification, verification and KYC procedures, including enhanced due diligence for those Dealing Entities presenting higher risk, such as Politically Exposed Persons (“PEPs”).
- 1.2 BMCP should not allow the opening or maintenance of any anonymous whitelist accounts in fictitious name or account on behalf of other persons whose identity has not been disclosed or cannot be verified.
- 1.3 The maintenance of appropriate records for the minimum prescribed periods.

2. INTERNAL CONTROLS

BMCP will develop and implement internal controls for the purpose of ensuring that all of its operations comply with AML legal requirements and that all legally required reports are made on a timely basis. Some of those internal controls are listed within this document and may include, but are not limited to, the Customer Identification Program, the Suspicious Activity Reporting system, and the required reports on the Policies' effectiveness to the Board, all of which are set out in the remainder of this Policies.

3. CUSTOMER IDENTIFICATION PROGRAM

- 3.1 The Customer Identification Program is to be carried out at the following stages: (i) while establishing a business relationship; (ii) before or during the carrying out of any financial transaction; and (iii) when there is any doubt about the authenticity/veracity or the adequacy of the previously obtained Dealing Entities' identification data.
- 3.2 BMCP will (i) require Dealing Entities to provide proof of identification; and (ii) not under any circumstances permit any transactions to be made with incomplete account-opening or background and identity verification information.
- 3.3 When there shall be any suspicion of money laundering or terrorism financing activities, or where there shall be any doubt about the adequacy or veracity of previously obtained Dealing Entities' identification data, the due diligence measures shall be reviewed, including verifying again the identity of the Participant and obtaining information regarding the purpose and intended nature of the business relationship with BMCP.

4. PROOF OF IDENTIFICATION & ID-VERIFICATION

- 4.1 For natural persons, sufficient identification data shall be obtained to verify:
 - First and Last name (it is going to be compared to the name provided on the identity picture required later)
 - Gender
 - Birthday date and place
 - Nationality
 - Phone number
 - National ID number
 - Sector of Activity
 - Social Security Number (provided only by US citizens)
 - Source of funds and source of wealth
 - Investment reason
 - Intended investment amount and currency.

- Politically exposed person (if checked, the user might need to provide additional information, depending on the specification of the issuer and his bank)
- Residential address
- Picture of an ID = the information on the ID is going to be compared with the information provided by the user above
- Proof of residence = has to be a bank statement or an utility bill addressed to the user
- verification of identity according to § 12 Geldwäschegesetz GwG (German AML laws)

4.2 For other legal entities, sufficient documentation shall be obtained to verify:

- Legal name of the company Registry number
- Legal form
- Incorporation date
- Sector of activity
- Registry country
- Legal address of the company
- Source of funds and wealth Investment reason
- Investment amount and currency
- LEI = Legal Entity Identifier or also Global business registry number
- Check for politically exposed persons in the company
- Information of the contact person in the company (see 4.1)
- Additional documents are going to be asked depending on the type of business the company is in and the legal structure. It may include:
 - o Evidence of Registration
 - o Incorporation documents
 - o Board Resolution to Invest
 - o Ownership structure (from counterparty to the natural person holding over 25%)
 - o Evidence of Regulation / stock listing
 - o List of beneficial owners
 - o Tax self-certification form
 - o Source of funds
 - o Source of wealth evidence
 - o Audited Financial Report
 - o Ultimate beneficial owner declaration
 - o Identity card of the beneficial owner
 - o Authorised signatories list
 - o Identity card of authorised signatories
 - o Shareholder register

5. SUSPICIOUS TRANSACTION AND ACTIVITY REPORTS

- 5.1 For the purpose of the Policies, a **“Suspicious Transaction”** means a transaction or attempted transaction, which to a person acting in good faith:

- gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
- appears to be made in circumstances of unusual or unjustified complexity;
- appears to have no economic rationale or bona fide purpose; and
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

5.2 Ongoing monitoring is an essential element of effective implementation. BMCP will diligently monitor transactions for Suspicious Transactions and other suspicious activity in relation to Token investments.

5.3 Internal controls will be implemented so that a monitoring system is in place to reasonably detect such activity as it occurs. When a suspicious activity is detected, BMCP's senior management and/or Compliance Officer will make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be filed. BMCP reserves the right to report suspicious transactions or activity to law enforcement authorities at its sole discretion.

5.4 BMCP will maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing. BMCP may inform BMCP's Board of the filing and the underlying transaction.

6. MAINTAINING RECORDS

6.1 Reasonable procedures for maintaining records of the information used to verify a person's name, address and other identifying information submitted for the purposes of participating in the sale of the DRG are required under this Policy. The following are required steps in the record keeping process:

- BMCP is required to maintain a record of identifying information provided by the Dealing Entities.
- Where BMCP relies upon a document to verify identity, BMCP must maintain a copy of the document that BMCP relied on that clearly evidences the type of document and any identifying information it may contain.
- BMCP must also record the methods and result of any additional measures undertaken to verify the identity of the Dealing Entities.
- BMCP must record the resolution of any discrepancy in the identifying information obtained.
- All transaction and identification records will be maintained for as long as legally necessary and to comply with applicable regulations.

- 6.2 All information collected from the Participants will be subject to BMCP's privacy policy, which is announced from time-to-time.

7. POST INVESTMENT ACTIVITIES AND ON AN ON-GOING BASIS

- 7.1 Establishing and maintaining the Policies towards assessing and managing the money and terrorist financing risks to BMCP.
- 7.2 Establishing and maintaining risk-based Dealing Entities due diligence, identification, verification and KYC procedures, including enhanced due diligence for those Dealing Entities presenting higher risk, such as Politically Exposed Persons.
- 7.3 Procedures for reporting suspicious fraudulent use of identification documents to the relevant law enforcement authorities as appropriate.
- 7.4 The maintenance of appropriate records for a reasonable period of time.
- 7.5 Providing appropriate management information and reporting to senior management of BMCP's compliance with the requirements of the Policies.
- 7.6 BMCP may require investors to provide additional information or documentation to fulfil our legal obligations and where it deems appropriate refuse any Participant or transaction that is suspected of being related to financial crime.