

KYC/CDD/CTF/AML Procedures and Policies

1. POLICY STATUS AND ACCEPTANCE

- 1.1. This KYC/CDD/CTF/AML Procedures and Policy (hereinafter referred to as the "Policy") sets forth the general rules and procedures governing the implementation and conduction of **Know-Your-Customer ("KYC")** procedures, **Customer-Due-Diligence (CDD)** and relevant **Counter-Terrorism Financing ("CTF") / Anti-Money Laundering rules ("AML")**.
- 1.2. Each User must carefully read and comply with this Policy. It is understood and presumed per se that by the fact of the Website use and Tokens purchase during a Token Sale or otherwise, the respective User fully read, understood and accepted this Policy. If any User does not agree with this Policy in general or any part of it, such User must not access and use the Website and/or purchase Tokens.
- 1.3. The Company reserves the right to modify or amend this Policy at its sole discretion. Any revisions to this KYC/CDD/CTF/AML Policy will be posted on the homepage of our Website. If we make changes, we will notify you by revising the date at the top of this Policy. We strongly recommend You to periodically visit the Website to review any changes that may be made to this KYC/CDD/CTF/AML Policy to stay updated on our KYC/CDD/CTF/AML practices. Your continued usage of the Website and/or services shall mean Your acceptance of those amendments.
- 1.4. In terms of a Token Sale this Policy shall be considered as inalienable part of a Token Sale Agreement, Our Privacy Policy and Terms of Use. In terms not regulated by this Policy, a Token Sale Agreement shall apply to the relationships that arise hereunder.
- 1.5. This Policy is administered by Chief Compliance Officer ("CCO") and the Compliance Department.



- 1.6. It is the personal obligation and responsibility of each Employee to act in a manner consistent with this Policy.
- 1.7. All Employees must report any breaches, violations, risks, incidents and complaints, as appropriate.

2. DEFINITIONS

- 2.1. **Applicable Law** – laws of (country): _____ applicable under this Policy to any and all relations between a User and Company.
- 2.2. **Employee** – a Company employee.
- 2.3. **Personal Information** - information or totality of information that can be associated with a specific person (the User) and can be used to identify that person. The rules governing the Personal Information collection, processing and use by the Company are documented in a separate Privacy Policy, which can be accessed via this [link](#) .
- 2.4. **KYC/CDD/CTF/AML Policy** (also referred to as **"Policy"**) – this KYC/ CDD/CTF/AML Policy posted on the homepage of our Website which may be revised or updated from time to time as stated in subsection 1.3 of this KYC/CDD/CTF/AML Policy.
- 2.5. _____ (**"Company", "Our", "Platform", "We", "Us"**) – a company incorporated under the legislation of (country): _____ for the purpose of Our project development and implementation, not being a financial entity, stock, exchange, investment entity or a partner, employer, agent or adviser for any User OR a third party, which we hire to perform services on our behalf such as Identity Verification.
- 2.6. The Platform is a is a blockchain-based economic platform bridging the gap between legacy, financial markets and emerging digital currency ecosystems.



- 2.7. **Token Sale ("Crowdsale")** – an offering of Tokens to eligible Users to purchase Tokens during the Sale Period, according to the respective phases (launches) and Token Price described on the Website and in Whitepaper.
- 2.8. **Token** – cryptographic tokens, which are software digital products (not being cryptocurrency), which are created by the Company and is a digital representation for participation in Our project, including the participation in distribution of Platform services and/or rewards
- 2.9. **User** (also referred to as "**You**") – any person, who uses the Website, with or without prior registration and authorization using their account and purchases of Tokens. The Company reserves its right to set forth at any time upon its own discretion special eligibility or other requirements to certain Users to participate in a certain phase of a Company's Token Sale as shall be mentioned on the Website and Whitepaper.
- 2.10. **Website** – the website maintained and owned by the Company at:

<https://bartertrade.io>
- 2.11. **Whitepaper** – one of the official Accompanying Documents published by the Company on the Website, describing technical and marketing details of the Token Sale, the idea and purpose of the Platform, as well as Token Price and Token Sale Period.

3. KYC/CDD/CTF/AML POLICY

- 3.1. We are strongly committed to preventing the use of its operations for money laundering or any activity which facilitates money laundering, or the funding of terrorist or criminal activities.
- 3.2. Regionally:
- 3.2.1. **Australia/New Zealand:** By establishing the 100-Point Check, AUSTRAC clearly defined a global standard for quantifying remote identity validation. And further AML/CTF



enacted by the Financial Transactions Reports Act (1988) (FTR Act), which established the Australian Transaction Reports and Analysis Centre (AUSTRAC) and which continues in existence under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

3.2.2. **European Union:** In order to prevent and combat money laundering and terrorism financing, there has been an introduction of the number of laws concerning the customer identification and verification procedures including but not limited to the EU AMLD5 Directive, which brings the virtual currencies under the scope of the Anti-Money Laundering Directive.

3.2.3. **United States:** regulation of the AML is carried out by a special government body under the US Treasury – FinCEN. In particular, FinCEN regulates, so-called, "money services business" (MSB). In 2013 FinCEN published the clarification on the regulation of persons administering, exchanging or using virtual currencies bringing the businesses dealing with virtual currencies under the scope of KYC/CDD/CTF/AML in terms of spotting suspicious financial behavior.

3.3. In order to ensure that our operations are compliant with the KYC/CDD/CTF/AML rules and procedures, we are implementing the KYC/CDD/CTF/AML policies detailed below.

3.4. As part of our AML (Anti-Money Laundering) Policy in order to combat money laundering and illegal financing activities the Company follows the customer risk assessment principles that include but are not limited to the following:

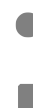
3.4.1. raise awareness on money laundering issues;

3.4.2. appoint a designated CCO. The CCO is to report any suspicious transactions to the appropriate Financial Authority;

3.4.3. assist law agencies and authorities to trace, seize, and confiscate the proceed of criminal activities;



- 3.4.4. freeze any funds deemed suspicious and investigate the source of finance;
 - 3.4.5. exercise reasonable measures to obtain information about the true identity of the persons on whose behalf a transaction is made;
 - 3.4.6. record keeping procedures – maintain, for a specific time period, all necessary records on transactions, both domestic and international;
 - 3.4.7. pay special attention to all complex, unusually large transactions;
 - 3.4.8. adopt economic, administrative, self-regulatory and other measures which can be taken to create an effective shield against money laundering;
 - 3.4.9. train staff accordingly;
 - 3.4.10. employ proper care in the hiring of new staff.
- 3.5. As part of the customer risk assessment, the following will act as Money Laundering Warning Signs based on guidance provided by Financial Action Task Force (FATF) – international body set up to combat money laundering:
- 3.5.1. customer tells that the funds are coming from one source but then at the last minute the source changes;
 - 3.5.2. evasiveness or reluctance to provide information;
 - 3.5.3. incomplete or inconsistent information;
 - 3.5.4. unusual money transfer or transactions (e.g. when customer deposits unusual amounts (e.g. 9,990 EUR) so as not to come under the threshold when KYC applies);
 - 3.5.5. complex group structures without obvious explanation that may be designed to disguise the true source and ownership of money;



- 3.5.6. when money is coming from the list of 'high-risk and non-co-operative jurisdictions' according to FATF;
- 3.5.7. negative public information available about the client or company.
- 3.5.8. Every Employee is required to act in furtherance of this policy statement to protect the Company from exploitation by money launderers or terrorists.
- 3.5.9. Company adopts the KYC (Know-Your-Customer) Policy and reserves the right to undertake KYC in order to verify the identity of its customers at any point.
- 3.5.10. As part of the exercise of this right, Company may require the following information to be sent:
 - 3.5.10.1. copy of passport or national ID;
 - 3.5.10.2. recent utility bill;
 - 3.5.10.3. recent bank account statement 'Recent' means no longer than 3 months from date of issue.
- 3.5.11. **Please note** that the list above is not exhaustive and we reserve the right to require additional information at any time to verify the client's identification and to fully satisfy the latest Anti-Money Laundering rules.
- 3.5.12. The Personal Information requested as part of the KYC procedure will be collected, processed, used and stored in accordance with the General Data Protection Regulation (GDPR), rules and principles of which have been reflected in the Company's Privacy Policy and implemented on the legal, technical and organizational level.
- 3.5.13. If any of the above documents are requested, prior to sending them to us we may require them to be certified as a true copy of the original by a Solicitor or a Lawyer who must use their company stamp. We require the documents to be sent to us in high quality color format. We reserve



the right to reject any documents, which do not comply with the above or if we have doubts as to their veracity.

- 3.5.14. If any doubt arises we reserve the right to check the information provided, as part of the KYC procedure, using non-documentary methods including but not limited to contacting the customer directly.
- 3.5.15. CCO has a right to freeze accounts and/or any funds already transferred should the suspicion as to the sources of those funds arises after they have been deposited and investigate the customer's transaction in retrospect.

4. KYC/CDD/CTF/AML Procedures

- 4.1. To ensure methodical diligence, we have implemented PCI-compliant document onboarding.
- 4.2. The Company offers two levels of KYC-compliant profile onboarding:
 - 4.2.1. Full (100-Point) KYC-Compliance, as defined:

Primary documents:

70 Points

Only one of the following may be claimed:

- Birth certificate
- Birth card issued by a Registry of Births, Deaths and Marriages
- Citizenship certificate
- Current passport
- Expired passport which has not been cancelled and was current within the preceding 2 years
- Other document of identity having the same characteristics as a passport including diplomatic documents and some documents issued to refugees



Secondary documents:**40 Points**

Document issued by Authorised Deposit-Taking Institutions (ADIs), banks, building societies, credit unions or registered corporations. Signatory is a known customer of at least 12 months standing.

Written reference from one of the following institutions, verifying name of signatory and signed by both referee and signatory. Signatory must be known for at least 12 months.

- Another financial body certifying that the signatory is a known customer
- Another customer who has been verified as a signatory by the cash dealer
- An acceptable referee (refer to AUSTRAC Guideline No. 3 and Information Circular No. 3 for applicable guidance)

Any of the following, which must contain a photograph and a name. Additional documents from this category are awarded 25 points.

- Government-issued Driver Licence
- Government-issued permit (e.g. a boat licence)
- Identification card issued to a public employee
- Government-issued Identification card issued as evidence of the person's entitlement to a financial benefit
- An identification card issued to a student at a tertiary education institution

35 Points

Name and address of signatory verified from any of the following:

- A document held by the cash dealer giving security over the signatory's property
- A mortgage or other instrument of security held by another financial body

Must have name and address on:

- A document held by a cash dealer giving security over your property
- A mortgage or other instrument of security held by a financial body
- Local government (council) land tax or rates notice



- Document from your current employer or previous employer within the last 2 years
- Land Titles Office record
- Document from licensed Credit Union

25 Points

Must have name and signature on:

- Marriage certificate (for maiden name only)
- Credit card
- Foreign driver licence
- health Care Card (Government-issued health care card)
- Membership to a registered club
- EFTPOS card

Must have name and address on:

- Government-issued Electoral Roll/List
- Records of a public utility - phone, water, gas or electricity bill
- Records of a financial institution
- A record held under a law other than a law relating to land titles
- Lease/rent agreement
- Rent receipt from a licensed real estate agent

○

Must have name and date of birth on:

- Record of a primary, secondary or tertiary educational institution attended by the applicant within the last 10 years
- Record of professional or trade association of which the applicant is a member.

4.2.2. "Safe Harbour" procedures for individuals with a medium or lower KYC/ML/TF risk, such as Ultimate Beneficiary Owners:

- customer's name; and
- either the customer's residential address, date of birth or that the customer has a transaction history of at least 3 years.

4.3. The Company relies on appropriate 3rd party services to assist with KYC, CDD and ML/TF efforts, as follows but not limited to:



- 4.3.1. **face-biometrically** measure the authenticity any/all documents provided to Us by the Customer - including, but not limited to:
 - 4.3.1.1. "Selfie"
 - 4.3.1.2. Passport, Driver's License, and other forms Government-issued IDs
 - 4.3.1.3. Student ID, and other non-Government IDs'
- 4.3.2. **Optical Character Recognition (OCR)** and **File Forensics (FF)** services to measure the authenticity any/all documents provided to Us by the Customer - including, but not limited to:
 - 4.3.2.1. Passport, Driver's License, and other forms Government-issued IDs
 - 4.3.2.2. Student ID, and other non-Government IDs
 - 4.3.2.3. Utility Bills
- 4.3.3. regularly (weekly) monitor our Customer-base for their individual associations to **"negative news"** by scanning (daily) nearly 500,000 licensed news articles - worldwide - in multiple languages, including but not limited to:
 - 4.3.3.1. English
 - 4.3.3.2. Spanish
 - 4.3.3.3. German
 - 4.3.3.4. Japanese
 - 4.3.3.5. Korean
- 4.3.4. regularly (weekly) monitor our Customer-base for their individual associations to "risk factors" or **"risk flags"** found on the global internet, and in other sources of **"public data"**.
- 4.3.5. authenticate Customer contact information via verified SMS.

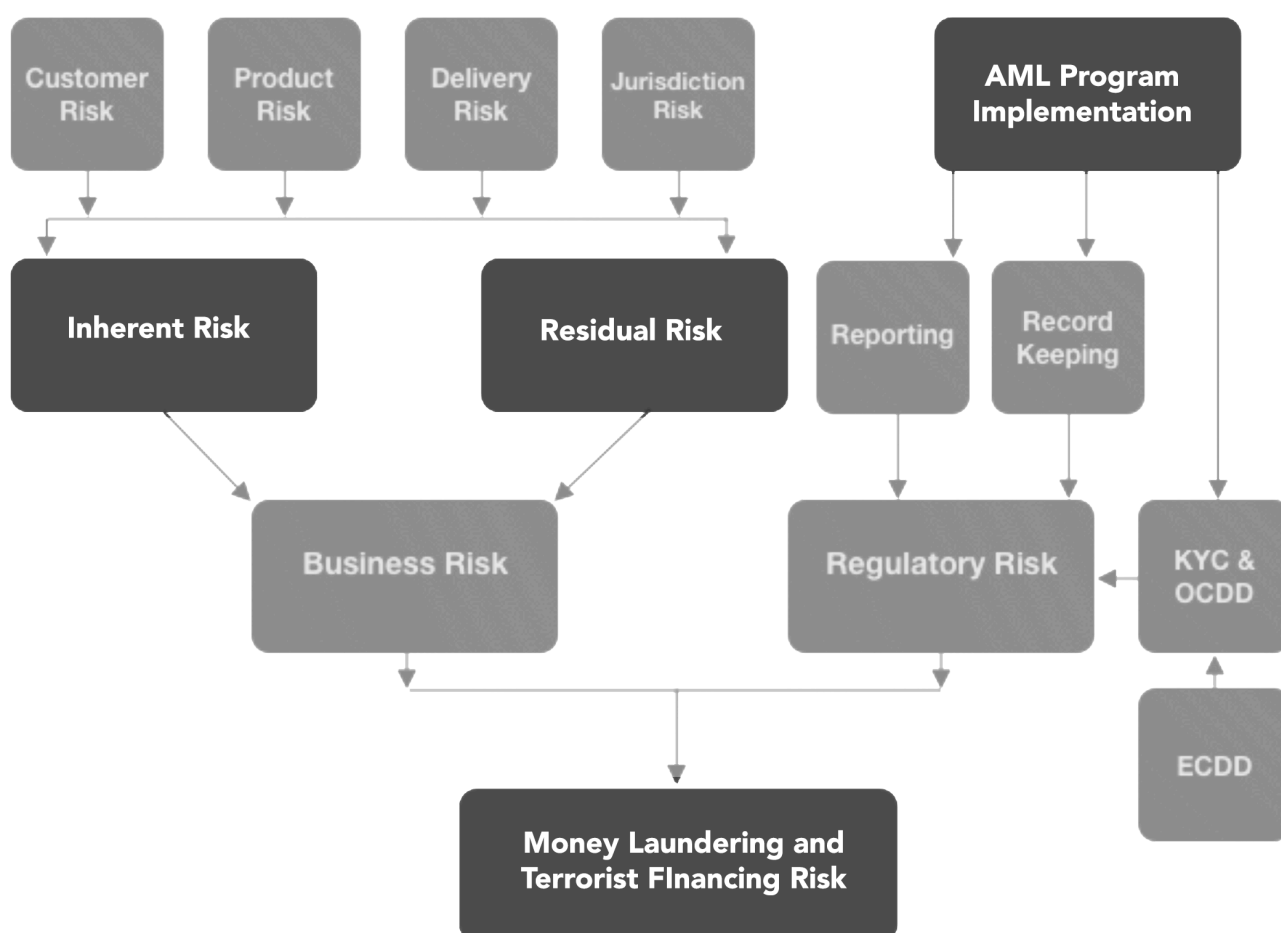


4.3.6. authenticate Customer identity claims via reverse telephone number lookup.

4.3.7. regularly (weekly) monitor our Customer-base against global **sanctions and watchlists**, which includes a current and global director of **Politically Exposed Persons** (PEPs). [APPENDIX: SANCTIONS & WATCHLISTS]

4.4. Any / all "flagged" Customers are delivered to the CCO for appropriate management, where the Company relies on an appropriate 3rd Party-driven back-office to closely assess and monitor our Customer-base.

4.4.1. Manual reviews are conducted in accordance with the outlined risk-based customer due diligence procedures:



- 4.4.2. whereby reporting entities should consider the risk posed by each of the following factors:
- 4.4.2.1. customer types, including beneficial owners of customers and PEPs
 - 4.4.2.2. customers' sources of funds and wealth (for example, by enquiring into the expected source and origin of the funds to be used in the provision of the designated service)
 - 4.4.2.3. nature and purpose of the business relationship (for example, the customer's business or employment)
 - 4.4.2.4. control structure of non-individual customers (for example, complex corporate structures and the underlying beneficial owners)
 - 4.4.2.5. types of designated services the reporting entity provides
 - 4.4.2.6. how the reporting entity provides its designated services (for example, over-the-counter or online)
 - 4.4.2.7. foreign jurisdictions in which the reporting entity deals (for example, customers that live or are incorporated in a foreign country).

4.5. Reporting

- 4.5.1. The Company has established a way in which its staff consults with their line managers to provide evaluation for the rationale of the further disclosure; by no means, this prevents contacting the nominated officer directly. All internal reports are registered in an appropriate way; the nominated officer maintains a secure suspicious report register.



4.5.2. The framework is created in such a way, where a reasonable and faithful evaluation is provided to each report that is received, for example:

●

■

SCAN DATE:
2019-06-06


AML
COMPLIANCE
REPORT

FOR
Judy Jane Doe

3rd-Party Verified Compliance URL:

KYC DILIGENCE


- Verified "Selfie"



- Verified SMS
- Verified Photo ID
- Validated Street Address
- Validated Bank Statement

NEGATIVE NEWS

none



AML DILIGENCE

DEA

FBI

ICE

Interpol

OFAC (SDN)

OFAC (Sanctions)

PEP

4.5.3. The nominated officer assesses the risk that is posed by a transaction or activity. In cases where there are associated accounts, an examination of such relationships is to be carried out. If an internal review has indicated enough grounds to know or suspect that any benefit has been acquired and if a criminal property exists, an external SAR report is submitted to NCA in a timely manner - not limited to:

4.5.3.1. AUS: <http://online.austrac.gov.au/>

4.5.3.2. EUR: <http://europa.eu/contact>

4.5.3.3. GBR: <https://www.fca.org.uk/markets/transaction-reporting>

4.5.3.4. USA: <https://www.fincen.gov/suspicious-activity-reports-sars>

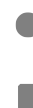
4.6. Record keeping

4.6.1. Records must be kept of all customers' identity, the supporting evidence of verification of identity (in each case including the original and any updated records), Our business relationship with them and details of any occasional transactions. As per regulatory requirements, we keep records for at least five years from the date a business relationship ends or from the date of the last transaction.

4.7. Training

4.7.1. We make sure that are employees are aware of our AML program and request that training is provided to all employees (new and existing) before conducting business activities, and, at a minimum, must include:

4.7.2. Understanding and recognizing money laundering and fraud
 Verifying customer identification
 Identifying suspicious activity and structured transactions
 Reporting requirements related to all transactions















- 4.7.3. Additional training should be provided regularly to all employees based on, but not limited to, changes in government regulations, The Company AML Compliance Program requirements, related procedures, and policies, or in the event of a performance issue related to an AML incident.

5. CONTACT DETAILS

- 5.1. If you have any questions regarding these KYC/CDD/CTF/AML Procedures and Policies, please contact us via email:



	APPENDIX - SANCTIONS & WATCHLISTS
	Australia Consolidated List (xl sheet)
	Australia most wanted
	Australia Crimestoppers
	OSFI Anti-terrorism Financing list
	Royal Canadian Mounted Police Wanted
	European Union financial sanctions list
	EU Members of Parliament
	Council of Europe's parliamentary assembly
	EEAS Consolidated List
	Eurpol
	EU Most wanted
	GB Insolvency Disqualified Directors
	GB Consolidated List of Targets
	Her Majesty's (HM) Treasury List
	World Bank Debarred Parties List CBI List (The Central Bureau of Investigation) India
	Japan Foreign End Users of Concern
	Kyrgyz FIU (State Financial Intelligence Service) National List
	Panama Company DB
	Swiss SECO Sanctions/Embargoes
	SDFM (Ukraine's financial intelligence) Blacklist
	Consolidated United Nations Security Council (UNSC) Sanctions List
	UN Consolidated Sanctions
	OFAC Specially Designated Nationals (SDN) list
	OFAC Foreign Sanctions Evaders (FSE) list
	Non-SDN Iranian Sanctions Act List (NS-ISA)
	Unverified List (UVL)
	Denied Persons List (DPL)
	The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List)
	Nonproliferation Sanctions
	BIS Entity List
	Palestinian Legislative Council (PLC) List
	Sectoral Sanctions Identifications (SSI) List
	AECA Debarred List
	Department of State Designated Foreign Terrorist Organizations
	Department of State Terrorist Exclusion List (TEL)
	Immigrations and Customs Enforcement Most Wanted Fugitives
	U.S. DEA Major International Fugitives
	U.S. Marshals Service Major Fugitive Cases
	U.S. Secret Service Most Wanted
	U.S. Marshals Service 15 Most Wanted
	FBI Most Wanted Terrorists
	U.S. Postal Inspection Service Most Wanted
	Naval Criminal Investigative Service Wanted Fugitives
	GB Consolidated List of Targets
	Bureau of Industry and Security
	FBI Top Ten Most Wanted CYBER
	Politically Exposed Persons (PEP) list
	International Criminal Police Organization (INTERPOL) List
	World Presidents Database
	CIA World Leaders
	INTERPOL Red Notices
	World Bank Debarred Parties List
	OCC Shell Bank List
	Panama papers database
	Exposing the Invisible