DCEX CUSTOMER DUE DILIGENCE PROCEDURES

Last Revision: **October 17, 2017**
Next Revision: **October 16, 2018**

Effective: **October 17, 2017**

1. Introduction

This DCEX LLC ("**DCEX**") Customer Due Diligence Policy and Procedures ("**CDD Policy**") details the processes by which DCEX satisfies regulatory Customer Due Diligence ("**CDD**") and Customer Identification Program ("**CIP**") requirements, and protects DCEX from the risks of financial crime.

DCEX regularly researches the relevant regulations and guidance on money laundering prevention and combating terrorist financing, and implements policies to ensure that its internal CDD procedures meet or exceed such requirements.

DCEX is required by the Bank Secrecy Act ("**BSA**") and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("**USA PATRIOT Act**") to implement and maintain a written CIP and CDD procedures to form a reasonable belief that DCEX knows the true identity of each of its customers.

DCEX operates an online business. The website ensures that customers provide the correct information at the first stage of client registration, and that clients provide additional information based on the amount they request to deposit or withdraw from DCEX's exchange platform.

DCEX has adopted a risk-based approach; all new clients must meet the requirements of DCEX's AML program. Clients not meeting these requirements will not be allowed to conduct business with DCEX.

Exceptions to the requirements are made only by the AMLO under the Exceptions Policy as detailed in Section 6 of this document.

2. Know Your Customer ("KYC")

It is paramount to understand each account as a whole, and to confirm that the use of each account makes sense. While the automated system performs most checks, Compliance, under the supervision of the AMLO, is responsible for ensuring DCEX knows its customers by documented evidence regarding each client.

Compliance is also responsible for monitoring each transaction to ensure that the account's purpose and use remain legitimate.

All employees are required to note anything that seems suspicious and escalate any questions to their manager or to Compliance.

2.1. Transaction Tiers and Information Collected

DCEX has implemented Know Your Customer ("**KYC**") procedures which require that DCEX obtain a sense of the legitimacy of funds sent, match the transaction to the sender's profile. DCEX maintains the following tiers based on the level of information the customer has provided.

Information on the below table is collected by DCEX's website prior to accepting any exchanges above the specified limits.

DCEX's website will attempt to obtain and verify all of the information below electronically. Prospective clients may not provide complete information online. Clients failing verification or providing incomplete information will not be able to transact.

Customer Tiers:

Tier	Requirements	Daily Limits (USD)	Monthly Limits (USD)
Tier 0	Account Sign-Up	*Fiat* Deposit: $0.00 Withdrawal: $0.00 *Cryptocurrency* Deposit: $0.00 Withdrawal: $0.00	*Fiat* Deposit: $0.00 Withdrawal: $0.00 *Cryptocurrency* Deposit: $0.00 Withdrawal: $0.00
Tier 1	1. Full Name 2. Birth Date 3. Address 4. Phone Number	*Fiat* Deposit: $0.00 Withdrawal: $0.00 *Cryptocurrency* Deposit: 2,999 Withdrawal: $2,999	*Fiat* Deposit: $0.00 Withdrawal: $0.00 *Cryptocurrency* Deposit: $20,000 Withdrawal: $20,000
Tier 2	1. All of the above 2. Address Verification (electronic) 3. Social Security Number (U.S. persons) or passport number (non-U.S. persons)	*Fiat* Deposit: $2,000 Withdrawal: $2,000 *Cryptocurrency* Deposit: Unlimited Withdrawal: $5,000	*Fiat* Deposit: $10,000 Withdrawal: $10,000 *Cryptocurrency* Deposit: Unlimited Withdrawal: $50,000
Tier 3	1. All of the above 2. Government issued ID 3. Verified proof of residence (<3 months old utility bill) 4. Social Security Number (US) 5. ID confirmation photo (selfie)	*Fiat* Deposit: $25,000 Withdrawal: $25,000 *Cryptocurrency* Deposit: Unlimited Withdrawal: $50,000	*Fiat* Deposit: $200,000 Withdrawal: $200,000 *Cryptocurrency* Deposit: Unlimited Withdrawal: $200,000
Tier 4	1. AMLO review and approval 2. Senior Management approval	*Fiat* Deposit: $100,000 Withdrawal: $100,000 *Cryptocurrency* Deposit: Unlimited Withdrawal: $100,000	*Fiat* Deposit: $500,000 Withdrawal: $500,000 *Cryptocurrency* Deposit: Unlimited Withdrawal: $500,000

2.2. Understanding Individuals

In conjunction with automated monitoring, Compliance ensures that accounts purposes and uses remain legitimate. Compliance may, in examining the totality of circumstances, question items such as:

- Are the amounts and types of exchanges requested in keeping with the stated purpose of the account?
- Is the client providing clear and concise answers to questions from Compliance?
- Is the amount of the exchange consistent with the client's profile and purpose of transfer, and does it seem reasonable?

Once a clear understanding of the client has been achieved, the activities that are conducted must make economic sense. Where a client's transactions appear uneconomic, a UAR should be submitted.

2.3. Risk Indicators for Sanction Breaches

Where any of the following indicators exist, the client should be contacted and asked to confirm that they will not send payments that involve any country listed as prohibited by DCEX.

- If the customer states the exchange is related to travel or services to or near to sanctioned countries;
- The customer is known to deal in:
    - Saffron;
    - Seeds;
    - Dried fruit;
    - Pistachios or other nuts;
    - Persian carpets;
    - Cigars; or
    - Minerals/ore.

2.4. Risk Indicators for Fraud and Money Laundering

Where any of the following indicators exist, file a UAR to notify Compliance:

Any concerns, suspicions, fears, gut feelings, feelings of discomfort, or unease regarding clients and their activities, including:

- Conducting business in or traveling to unusual jurisdictions;
- Email addresses containing the client's year of birth i.e. Donald.Duck1980@hotmail.com;
- Email address that do not reflect the client's name. E.g. account holder: Donald Duck, email address: Mickey.Mouse@hotmail.com;
- Unable to connect to the telephone number(s) supplied;
- A third party answering the phone who does not know of the client;
- Email addresses not working;
- A number of accounts bearing similar data that may be connected;
- IP address far from the client's address;

- Google street view of the client's address indicates a residence that may not correspond to the exchange size;
- Unusually high volumes of transactions;
- Urgency on behalf of the client to complete the trade;
- Client's accent or voice does not match the nationality or age that is stated on the account;
- Multiple transactions booked in quick succession;
- Transactions that appear unusual in their nature – ensure the purpose of transfer is understood;
- Transactions that appear uneconomic;
- Is the client acting in accordance with how you would expect them to act?
    - Are frequencies and volumes in line with expectations for their personal needs and/or in accordance with the purpose initially indicated to DCEX?
    - Are they operating in markets relevant to their personal circumstances?
- Any other client activity that does not make sense.

This list should be continually reviewed and updated as and when new indicators emerge. It is important to remember that there may be a sufficient reason for some of the above indicators. Ensure you have conducted as much independent research as possible prior to contacting the client. This may include reviewing the account as a whole, reviewing previous payments, conducting internet searches, etc.

3. US Private Individuals Customer Due Diligence

3.1. Electronic Verification

Customers are verified using IdentityMind, an external vendor, which applies the following checks to each new account. These checks both verify a client's identity and suggest whether that client may present an increased risk of criminal activity:[1]

- Economic Sanction and Related Screening. The client's name, date of birth, and residence is matched against the following lists:

  PEP: US Ambassadors
  OSFI Anti-terrorism Financing list
  PEP: Diplomatic
  PEP: Detailed PEP Information
  Non-SDN Iranian Sanctions Act List (NS-ISA)
  Canadian Judges
  Consolidated United Nations Security Council (UNSC) Sanctions List
  PEP: Global 500
  PEP: CIA
  SEC Sanctions Database
  Canadian Mayors
  PEP: Most Powerful in Finance
  PEP: Top 100 Hedge Funds Key Principals
  U.S. DEA Major International Fugitives
  OFAC Specially Designated Nationals (SDN) list
  Royal Canadian Mounted Police - Wanted
  AECA Debarred List
  U.S. Secret Service Most Wanted
  Nonproliferation Sanctions
  PEP: Active
  SWISS Sanctions
  Department of State Designated Foreign Terrorist Organizations
  U.S. Marshals Service Top 15 Most Wanted
  Canadian Politicians Family
  Denied Persons List (DPL)
  PEP: Bank Members
  PEP: Whitepages
  PEP: UN Representatives
  U.S. Postal Inspection Service Most Wanted
  Palestinian Legislative Council (PLC) List
  PEP: Mayors
  Unverified List (UVL)
  FBI Most Wanted Terrorists
  PEP: Foreign Consular List

[1] This list of verification measures is current as of this document's publication. The Compliance Officer may adjust these from time to time in order to provide the most effective onboarding and KYC process.

Entity List
International Criminal Police Organization (INTERPOL) List
OFAC Consolidated Sanctions list
PEP: Known Associates
PEP: Congress
PEP: Supreme Court Justices
European Union financial sanctions list
Israeli Sanctions
The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List)
Sectoral Sanctions Identifications (SSI) List
Naval Criminal Investigative Service - Wanted Fugitives
Immigrations and Customs Enforcement Most Wanted Fugitives
PEP: Governors
PEP: World Leaders
PEP: Mexican Politicians
UK Consolidated list of targets
PEP: Mexico
PEP: US Top Political Donors
Japan Foreign End Users of Concern
Politically Exposed Persons (PEP) list
Department of State Terrorist Exclusion List (TEL)
Canadian Military
U.S. Marshals Service Major Fugitive Cases

The Company has elected to match these lists at 100% name match. Mitek Instant Document Verification, described below, ensures name and date of birth data is accurately captured.

- Mitek Instant Document Verification. This service captures a user's identification using their mobile device and processes the image and metadata gathered from the image to validate that the document appears genuine, unaltered, and is valid. For additional verification, if necessary, this service can also use a "selfie" to further match the customer to the documents submitted.

- Device Count. Reports whether the device used to register has been seen before, and if so, the number of occurrences.

- Email Reputation. The Company will screen for known disposable email domains as well as suggest the reputability of an email address based on its prior use in available sources.

- Bot Check. Reports whether traffic appears to be coming from an automated "bot" or a real person.

- Device Reputation. Reports whether a device used to register with the Company has been detected as used in other questionable transactions.

- Tor Browser. Detects whether traffic appears to be coming from the Tor anonymous browsing network.

- Proxy Check. Detects whether traffic appears to be coming from a proxy network.

- Timezone Mismatch. Detects whether there is a timezone mismatch between reported and detected locations.

- IP Geographical Checks. Detects whether the customer's IP address may indicate the customer is not logged in from their reported address.

- Address Reputation. Reports whether an address used to register with the Company has been detected as used in other questionable transactions.

- KYC Velocity and User Checks. Reports whether, based on device, IP, or other reliable indicia, any user may have applied for more than one account over a short period of time. Also detects other accounts that may be associated with a single user or device.

- Watchlist. Reports whether a customer appears on the Company's internal watchlist or may be associated with a high risk geography.

- Blacklist. Reports whether a customer appears on the Company's internal blacklist or may be associated with a restricted geography such as a sanctioned country.

3.2. Risk Ratings

DCEX generates an initial risk rating for new accounts. This initial rating is only a guide, and may not represent the account's true risk. Risks highlighted by the risk rating system provide useful information.

Complete the following additional steps for each account based on the automatic risk rating generated, and any observations that indicate the account may be higher risk.

The Risk-Based Approach for U.S. Individuals	
Low	High
Complete basic client verification measures.	Complete basic client verification measures.
	If the client is a politically exposed person ("PEP") (always high risk) then paper-based verification on source of funds and source of wealth is required. A PEP should be signed off by the AMLO. A PEP with known connections to high risk jurisdictions must also be signed off by a member of the board.
Basic transaction monitoring.	Increase transaction monitoring or decline business.
Place on 5 Year Review Schedule.	Place on 1 Year Review Schedule.

4. Global Considerations

DCEX, and its affiliates, may operate in multiple jurisdictions. Therefore, Compliance must be aware of certain situations that may implicate more than one jurisdiction.

4.1. Account Transfers

When a client's residence moves into a jurisdiction in which another affiliated entity operates, the account in the old jurisdiction must be closed and a new relationship must be established in the new jurisdiction.

For example, a United Kingdom client moves permanently to the US. The client must have its transfers monitored by Compliance, adhering to this AML Program, and therefore a new relationship in the U.S. must be established.

4.2. Temporary Residence

Individuals temporarily in the United States are not exempt from identification requirements and will not be able to transact unless they are able to pass verification as if they were a permanent U.S. resident.

4.3. Documents in Foreign Languages

If a document is written in a foreign language, and there are no DCEX employees able to translate that language, refer the document to the AMLO.

5. Periodic Review of Accounts

All new accounts are placed on a schedule for periodic review. The frequency of such reviews depends upon the risk rating of the account. Any account without any activity in the previous year may be excluded from the periodic review until the next time the account becomes active, at which time the review must take place before transactions can be processed.

5.1. Review Schedule

Low Risk Accounts	Every 5 years
High Risk Accounts	Every year

5.2. Review Process

Compliance will review accounts by completing and saving a High Risk Accounts Review Checklist ("**Checklist**").

This Checklist includes fields for whether the following information has remained the same or changed:

- Exchange volume;
- Exchange frequency;
- Exchange tokens or currencies;
- Source of funds; and
- Fraud indicators.

The Checklist also includes sections for comments, initial and post-review risk, any updates made to the account or UARs submitted due to changed information, and whether enhanced due diligence may be required.

6. Exceptions to this CDD Policy

All exceptions to the CDD Policy must be effected in accordance with the following procedure:

In certain circumstances it may be reasonable to deviate from the CDD Policy. In order to do so, the AMLO must document the exception in the Compliance Log along with the reasons why the exception is being made and the name of person making the exception.