# Anti-Money Laundering Policy

The objective of Anti-Money laundering procedures that Zurich Prime implements is to ensure that customers engaging in certain activities are identified to a reasonable standard, while minimizing the compliance burden and impact on legitimate customers.
Money laundering is the act of converting money or other monetary instruments gained from illegal activity into money or investments that appear to be legitimate, so that its illegal source cannot be traced. Domestic and international laws that apply to companies, whose customers can deposit and withdraw funds from their accounts, make it illegal for the company, or its employees or agents, to knowingly engage, or attempt to engage in a monetary transaction of criminally derived property.

## Implemented Procedures

The objective of Anti-Money laundering procedures that U-NEX SOLUTIONS SRL implements is to ensure that customers engaging in certain activities are identified to a reasonable standard, while minimizing the compliance burden and impact on legitimate customers. U-NEX SOLUTIONS SRL is committed to assisting governments combat the threat of money laundering and financing terrorist activities around the world. For that purpose U-NEX SOLUTIONS SRL has set up a highly sophisticated electronic system. This system documents and verifies client identification records, and tracks and maintains detailed records of all transactions.
U-NEX SOLUTIONS SRL carefully tracks suspicious and significant transaction activities, and reports such activities “providing timely and comprehensive information” to law enforcement bodies. To uphold the integrity of reporting systems and to safeguard businesses, the legislative framework provides legal protection to providers of such information.
In order to minimize the risk of money laundering and financing terrorist activities, U-NEX SOLUTIONS SRL neither accepts cash deposits nor disburses cash under any circumstances. U-NEX SOLUTIONS SRL reserves the right to refuse to process a transfer at any stage, where it believes the transfer to be connected in any way to money laundering or criminal activity. It is forbidden for U-NEX SOLUTIONS SRL to inform customers that they have been reported for suspicious activity.

ZURICH PRIME

# Additional Disclosures

## CUSTOMER DUE DILIGENCE

Effective Customer Due Diligence (”CDD”) measures are essential to the management of money laundering and terrorist financing risk. CDD means identifying the customer and verifying their true identity on the basis of documents, data or information both at the moment of starting a business relationship with customer and on an ongoing basis. The customer identification and verification procedures require, first, the collection of data and, second, attempts to verify that data.
Appropriate documents for verifying the identity of customer include, but are not limited to, the following:

- Customer verification documents: Passport or national identification card together with a current valid utility bill.
- Credit Card verification documents: Copy of both sides of credit card displaying the last four digits of the card and the expiry date. Additionally, Customers are required to confirm every credit card transaction by signing the Company credit card deposit declaration (received by email, immediately after a new transaction was performed)

If an existing customer either refuses to provide the information described above or if a customer has intentionally provided misleading information, the Company, after considering the risks involved, will consider:

- Closing any of an existing customer’s accounts
- Obtaining the information relating to the source of the funds or the wealth of the customer will be required (this will be done via e-mail or phone)
- Seek further information from the customer or from Company’s own research and

Third party sources in order to clarify or update the customer’s information, obtain any further or additional information, clarify the nature and purpose of the customer’s transactions with Company.
When obtaining information to verify the customer’s statements about source of funds or wealth, the Company’s staff will most often ask for and scrutinize details of the person’s employment status or business/occupation. The Company’s staff will ask for whatever additional data or proof of that employment/occupation that may be deemed necessary in the situation, particularly the appropriate confirming documents (employment agreements, bank statements, letter from employer or business etc.).
The Company will conduct ongoing customer due diligence and account monitoring for all business relationships with customers. It particularly involves regularly reviewing and refreshing Company’s view of what its customers are doing, the level of risk they pose, and whether anything is inconsistent with information or beliefs previously held about the customer. It can also include anything that appears to be a material change in the nature or purpose of the customer’s business relationship with

## Use of Information

By registering an account with the Company, you consent to the use of your personal details, and their processing: collection, recording, classification, aggregation, storage (updating, changing) extraction, use, transfer (distribution, provision of access) anonymization, blocking, deletion, and destruction of any information relating directly or indirectly to you, your trade transactions and payments, in accordance with our Privacy Policy (http://zurichprime.com/privacy-policy/ )

## Payout Policy - Deposits and Withdrawals

Please be aware that chargebacks to bank cards are prohibited. To make a withdrawal from a trading account to your bank card, a correspondent request must be submitted via the Cashier.
U-NEX SOLUTIONS SRL requires all deposits, where the name of the originating customer is present, to come from the name matching the name of the customer in our records. Third party payments are not accepted.
As for withdrawals, money may be withdrawn from the same account and by the same way it was received. For withdrawals where the name of the recipient is present, the name must exactly match the name of the customer in our records. If the deposit was made by wire transfer, funds may be withdrawn only by wire transfer to the same bank and to the same account from which it originated. If the deposit was made by means of electronic currency transfer, funds may be withdrawn only by the means of electronic currency transfer through the same system and to the same account from which it originated.
If you have any inquiries, please contact us via e-mail: Support@ZurichPrime.com

## AML Compliance Officer

The Company shall appoint an AML Compliance Officer, who will be fully responsible for the Company's AML and CFT program and report to the Board of the Company or a committee thereof any material breaches of the internal AML policy and procedures and of the Regulations, codes and standards of good practice.

## AML Compliance Officer's responsibilities include:

a)Ensuring the Company's compliance with the requirements of the Regulations;
b)Establishing and maintaining internal AML program;
c)Establishing an audit function to test its anti-money laundering and combating the financing of terrorism procedures and systems;
d)Training employees to recognize suspicious transactions;
e)Receiving and investigating internal suspicious activity and transaction reports from staff and making reports to the FIU where appropriate;
f)Ensuring that proper AML records are kept;
g)Obtaining and updating international findings concerning countries with inadequate AML systems, laws or measures.

## Employees

All Company employees, managers and directors must be aware of this policy.
Employees, managers and directors who are engaged in AML related duties must be suitably vetted. This includes a criminal check done at the time of employment and monitoring during employment.
Any violation of this policy or an AML program must be reported in confidence to the AML Compliance Officer, unless the violation implicates the AML Compliance Officer, in which case the employee must report the violation to the Chief Executive Officer.
Employees who work in areas that are susceptible to money laundering or financing terrorism schemes must be trained in how to comply with this policy or the AML program. This includes knowing how to be alert to money laundering and terrorism financing risks and what to do once the risks are identified.

## Employee Training Program.

The Company provides AML training to employees who will be dealing with customers or will be involved in any AML checking, verification or monitoring processes. The Company may conduct its training internally or hire external third party consultants.
Each person employed within the Company is assigned a supervisor who teaches him or her in relation to all policies, procedures, customer documentation forms and requirements, forex markets, trading platforms, etc. There is a training plan for each new employee and tests which are being held for 2-3 months (depending on level within the business).
The Company's AML training programs is aimed to ensure its employees to receive appropriate training level with regards to any possible AML/TF risks.

## Content of training

The Company's AML and risk awareness training includes the following content:

- The Company's commitment to the prevention, detection and reporting of ML and TF crimes.
- Examples of ML and TF that have been detected in similar organizations, to create an awareness of the potential ML and TF risks which may be faced by the Company's employees
- Well known or recognized typologies, especially where made available by the FATF or AML Supervisors.
- The consequences of ML and TF for the Company, including potential legal liability.
- The responsibilities of the Company under the AML Act and Regulations.
- Those particular responsibilities of employees as identified in this AML Policy, and how employees are expected to follow the Company's AML procedures.
- How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.
- The rules that apply against unlawful disclosure of suspicious transactions ("tipping off").