



uexo \ WealtLink (PTY) Ltd. \ FSCA

Anti-Money Laundering Policy

v1.2

Table of Contents

1. Introduction	3
2. Definition of Money Laundering	4
3. Company's Procedures	6
4. KYC and CDD	7
5. Individual Clients	8
6. Corporate Clients	10
7. Additional Provisions	11
8. Regional Restrictions	12
9. Monitoring of Clients Activities	13
10. Deposit and Withdrawal Requirements	14
11. What is Counter Terrorist Financing (CTF)?	15
12. Record Keeping	16
13. Activity Monitoring	17
13.1 Suspicious Activity	17
13.2 Know Your Customer – The Basis for Recognising Suspicions	18
13.3 Suspicious Scenarios	18
13.4 Reporting a Suspicion	19
13.5 Investigation	19
13.6 Freezing of Accounts	19
Do you have any questions?	20

1. Introduction

The uexo brand is authorised and regulated in various jurisdictions, with the South African entity being owned and operated by Wealthlink (PTY) Limited. Wealthlink (PTY) Ltd. (hereinafter referred to as "uexo," or "Company" from this point on) has its address at 5th Street, Atrium On 5th, 9th Floor, Sandhurst, Johannesburg, 2196, South Africa. The company is authorised and regulated by the Financial Sector Conduct Authority in South Africa (FSCA) under the licence FSP number 50582 and has the CIPC company number 2019 / 514704 / 07.

2. Definition of Money Laundering

Money Laundering is the process of converting funds, received from illegal activities (such as fraud, corruption, terrorism, etc.), into funds or investments which look legitimate to hide or distort the real source of funds.

The process of money laundering can be divided into 3 sequential stages:

★ **Placement.**

At this stage funds are converted into financial instruments like checks, bank accounts, money transfers or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency exchangers). To avoid suspicion by the company, the launderer may as well make a number of deposits instead of depositing the whole sum at once; this form of placement is called smurfing.

★ **Layering.**

Funds are transferred or moved to other accounts or converted into other financial instruments. It is aimed at disguising the origin of funds and distorting the trail by conducting multiple financial transactions. Moving funds around and changing their form makes it complicated to trace the money being laundered.

★ **Integration.**

Funds get back into circulation as legitimate and can be used to make purchase of goods and services.

Like the majority of companies providing services in the financial markets, uexo adheres to principles of Anti-Money Laundering (hereinafter referred to as "AML") and actively prevents any actions that aims or facilitates the process of legalisation of illegally gained funds.

AML policy means preventing the use of the Company's services by criminals, with the aim of money laundering, terrorist financing or other criminal activity. For this purpose, a strict policy on the detection and prevention of any suspicious activities and reporting to the corresponding regulatory bodies was introduced by the Company. Moreover, the Company has no right to report to Clients that the law enforcement bodies are informed on their activity. A complex electronic system for identifying all of uexo's Client's has also been introduced. These systems conduct detailed monitoring of all operations.

To prevent money laundering, the Company neither accepts nor pays cash under any circumstances. The Company reserves the right to suspend any Client's operation, which can be regarded as illegal or, may be related to money laundering in the opinion of the Company.

This AML policy shall be communicated to all the employees of the Company that manage, monitor or control in any way the client's transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

This AML policy also applies to all Company's officers, appointed contractors, agents, products and services offered by the Company. All business units within the company will cooperate to create a cohesive effort in the fight against money laundering.

The appropriateness, effectiveness and adequacy of this AML policy are the subject of an independent Internal Audit.

3. Company's Procedures

The Company will make sure that it is dealing with a real person or legal entity. The Company also performs all the required measures in accordance with applicable laws and regulations, issued by the relevant supervisory authorities. This AML policy is being fulfilled within the Company by means of the following:

- ★ Know Your Customer, which is also referred to as KYC, and Customer Due Diligence, which is referred to as CDD.
- ★ Ongoing Monitoring of Client's activities.
- ★ Record Keeping.

The Company assesses and evaluates the risks it faces based on various criteria, including but not limited to the Client's nature, Client's behaviour, Client's initial communication with the Company, as well as the risks based on the Company's services and securities.

4. KYC and CDD

Due to the Company's commitment to the AML and KYC policies, each Client of the Company has to finish the verification procedure. Before the Company starts any cooperation with the Client, the Company must ensure that satisfactory evidence is produced, or such other measures are taken as will produce satisfactory evidence of the identity of any Client or counterparty.

The Company as well applies heightened scrutiny to Clients, who are residents of the countries, identified by credible sources as countries, having inadequate AML standards or may represent high risk for crime and corruption and to beneficial owners who reside in and whose funds are sourced from named countries.

5. Individual Clients

During the process of being onboarded via the registration process, each Client provides personal information, specifically the following information:

- ★ Full name
- ★ Date of birth
- ★ Country of birth
- ★ Residential address
- ★ Phone number (including the international and/ or city code)
- ★ Other information the Company deems necessary

Individual Client's shall also provide the following documents (in case documents are written in non-Latin characters, to avoid any delays in the verification process, it is necessary to provide a notarised translation of the document into English) because of the requirements of KYC and to confirm the indicated information. These documents can include any of the following, given that they are not expired:

- ★ Valid passport
- ★ National ID card
- ★ Driver's licence
- ★ Any other government-issued identification document.

The indicated documents should contain the Client's full name (and the name should be identical to the name on the document as well as the name given by the Client during the onboarding phase), date of birth, photo, and citizenship of a Client, and also, where applicable, confirmation of the document validity (issue and/or expiry date), as well as the holder's signature.

The indicated documents must be valid at the time of submission and for at least thirty (30) days from the submission date.

For the purposes of the provisions relating to identification procedures and CDD requirements, proof of identity is satisfactory if:

- ★ It is reasonably possible to establish that the Client is the person he claims to be and,
- ★ The person who examines the evidence is satisfied, in accordance with the procedures followed under the relevant legislations and regulations that the Client is actually the person he or she claims to be.

The current residential address shall be verified by one of the following things, which have to be dated within the last three (3) months:

- ★ A recent utility bill, such as a gas, water, telephone, internet, or electricity bill
- ★ A Bank statement
- ★ Credit card statement
- ★ Tax Clearance or Tax Return
- ★ Insurance Policy

- ★ Police Character Certificate
- ★ Affidavit
- ★ Certificate of Residence or Residence Permit in case if aforementioned documents contain the current residential address and name of the client
- ★ Valid passport, national ID card, or driver's licence which contains the current residential address and name of the client and in countries/regions where this is specifically allowed
- ★ Any other government-issued document that contains the current residential address and name of the client.

As stated above, any utility bill, bank statement, or credit card statement should not be older than three (3) months from the submission date. For the other documents, there is no prescribed time frame, however, the documents must be current and not expired.

Where certification is required, the documents should be certified by either one of the following:

- ★ An attorney
- ★ A lawyer
- ★ A notary
- ★ An actuary
- ★ An accountant
- ★ Any other person holding a recognised professional qualification, director or secretary of a regulated financial institution in South Africa or meets the FATF's standards, a member of the judiciary or a senior civil servant.

Both sides of the submitted document are required where applicable, for example, both sides of an ID or a driver's licence are required. The image of the document must be a colour high-resolution photo or scan copy with no blurs, light reflections, or shadows. Four edges of the document should be visible. All information should be clearly readable, free of any watermarks, etc.

For each account, the Company shall also make reasonable effort, prior to the settlement of the initial transaction, to obtain the following information to the extent it is applicable to the account:

- ★ Occupation of the Client
- ★ The Client's investment objective and other related information concerning the Client's financial situation and needs
- ★ Annual income, assets or net worth
- ★ Other information the Company deems necessary for opening an account.

6. Corporate Clients

In case the applicant company is listed on a recognised or approved stock exchange or where there is independent evidence to show that the applicant is a wholly owned subsidiary or subsidiary under the control of such a company, no further steps to verify identity will normally be required.

In case the company is unquoted and none of the principal directors or shareholders already has an account with the Company, the official provides the following documents because of the requirements of KYC:

- ★ Copies of the Certificate of Registration/Certificate of Incorporation
- ★ Copies of the Memorandum and Articles of Association, Partnership Agreement or similar, as appropriate
- ★ Copies of the By-Laws and latest General Information Sheet, which lists the names of directors/partners and principal stockholders, and secondary licences
- ★ Extract from Commercial Register, or equivalent document, proving the registration of corporate acts and amendments and current state of the legal person such as Certificate of Good Standing
- ★ Copy of the Certificate of Incumbency issued not older than 3 months from the filing date
- ★ Information about the BOs of the company from the independent and reliable sources
- ★ KYC documents of all Directors, Shareholders, BO's and Officers of the legal person where applicable
- ★ Appropriate Board of Directors' resolutions and signed application forms or account opening, identifying the authorised signatories or principal officers of the corporation authorised to open an account, to trade and their authorities and specimen signatures
- ★ Evidence of the registered address and actual place of business of the legal person
- ★ Latest Audited Financial Statements (if applicable)
- ★ Where applicable, the Company may also require additional information about the nature of the business of Clients such as the description and nature of business (including date of commencement of business, products or services provided, principal place of business).

In view of adopting the risk based approach, any Client who deposits an equivalent amount of USD \$15,000 or more must also provide relevant documentary evidence (pay slips, letter of confirmation from current Employer, or in the case of Institutional Clients, Audited Financial Statements, or Management Accounts) along with the Declaration of the Source of Fund/Source of Wealth.

This procedure is performed to establish the identity of the Client and to help the Company know/understand Clients and their financial dealings to be able to provide the best services of online trading.

7. Additional Provisions

If, during the business relationship, the Client fails or refuses to submit, within a reasonable timeframe the required verification data and information, the Company shall terminate the business relationship and close all the accounts of the Client.

Customer Due Diligence regarding the Individual Clients, as well as Corporate Clients shall be updated and/or amended soon after any changes take place. This refers to change of residential or business address, new identification cards, new passport, additional business information, new business securities/venture, and the like. For any change of information before the said period the Company requests a letter or document pertaining to the changes being made.

When accepting new Clients during the verification process and documents review, the Company reserves the right to apply other requirements and procedures for the Client's identification. Such procedures are to be determined at the Company's sole discretion and subject to variations depending on various factors, including but not limited to the country of residence of the Client, Client's profile and others. The Company can request the Client to provide a source of funds, source of wealth documents, proof of funds being deposited in a form and manner as the Company finds appropriate and other documents the Company deems necessary to complete verification procedure.

8. Regional Restrictions

uexo recognizes the importance of complying with international regulations and regional restrictions to ensure the legality and security of our services. While we strive to offer our services to a global audience, there are specific regional restrictions that may impact access to and use of our platform. Customers are advised to take note of the following restrictions and obligations when accessing uexo services from the following countries:

- ★ Afghanistan
- ★ Belarus
- ★ Burma
- ★ Central African Republic
- ★ Cuba
- ★ Democratic Republic of Congo
- ★ Ethiopia
- ★ Iran
- ★ Iraq
- ★ Syria
- ★ Lebanon
- ★ Libya
- ★ Mali
- ★ Nicaragua
- ★ North Korea
- ★ Russian Federation
- ★ Somalia
- ★ South Sudan
- ★ Ukraine
- ★ Venezuela
- ★ Yemen
- ★ Zimbabwe
- ★ The United States of America

9. Monitoring of Clients Activities

In addition to gathering information from the Clients, the Company continues to monitor the activity of every Client to identify and prevent any suspicious transactions. A suspicious transaction is known as a transaction that is inconsistent with the Client's legitimate business or usual Client's transaction history known from the Client activity monitoring. The Company has implemented the system of monitoring the named transactions (both automatic and manual) to prevent the use of the Company's services by criminals.

The Company reserves the right to suspend any Client's operation, which can be regarded as illegal or, may be related to money laundering in the opinion of the staff.

The constant monitoring of the Client's accounts and transactions is an imperative element in the effective control of the risk of Money laundering.

10. Deposit and Withdrawal Requirements

All the Clients' operations to deposit and withdraw funds have the following requirements:

- ★ In the case of a bank transfer or a transfer from the bank card of the Client, the name of the Client (which needs to be identical to the Client's name the Client used during the registration phase) must match the name of the owner of the account/bank card. It is possible to withdraw funds from the account via bank transfer only in the same bank and the same account which you used for depositing.
- ★ In the case of using electronic payment systems, withdrawing funds from the uexo trading account is possible only on the system and the account used for depositing.
- ★ If the account was credited in the way that cannot be used for funds withdrawal, the funds may be withdrawn to a bank account of the client or any other way may be used, as agreed with the Company with the condition that the Company is able to prove the identity of the account owner.
- ★ If the account has been credited with funds through various payment methods, funds withdrawal shall be made on a pro rata basis, which commensurate to the size of each deposit. Any profit gained can be transferred to any account from which the deposits arrived as long as such transfer is possible.
- ★ If the account has been credited using various payment methods and one of such methods was a bank card(s), the Company shall only process withdrawal requests to such a bank card(s) until up to the total amount of initial deposit using the bank card(s) is withdrawn before allowing to create any withdrawal requests via other payment methods and withdrawal of profit gained.
- ★ No deposits and withdrawals to the bank accounts, bank cards, electronic money, or any other kind of payment accounts of third parties are allowed

11. What is Counter Terrorist Financing (CTF)?

Terrorist financing refers to the practice of legitimate entities and individuals offering financial support to further terrorist activities or organisations driven by ideological, political, or various motivations. It is essential for organisations to ensure two key aspects: (i) that their customers are not affiliated with terrorist organisations, and (ii) they do not inadvertently facilitate the funding of such organisations.

Terrorist financing may not necessarily involve the proceeds of criminal activities. Instead, it often entails efforts to obscure the source and intended purpose of the funds, with the ultimate aim of utilising them for unlawful activities.

12. Record Keeping

Records will be kept for all documents obtained for the purpose of Client's identification (AML Policy requirements) and all information of each transaction, as well as other information related to the Client received in accordance with the applicable AML laws/regulations.

The following document retention periods will be followed:

- ★ All documents in opening the accounts of Clients and records of all their transactions, especially Client's identification records, shall be maintained and safely stored for seven (7) years from the dates of transactions
- ★ With respect to closed accounts, the records on Client's identification, account files and business correspondence, shall be preserved and safely stored for at least seven (7) years from the dates when they were closed.

13. Activity Monitoring

Transaction based monitoring will occur within the appropriate business units of uexo. Monitoring of specific transactions will include but is not limited to transactions aggregating \$5,000 or more and those with respect to which uexo has a reason to suspect suspicious activity. All reports will be documented.

13.1 Suspicious Activity

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as 'red flags'. If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee.

Examples of red flags are:

- ★ The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspect identification or business documents.
- ★ The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business strategy.
- ★ The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- ★ Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- ★ The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- ★ The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- ★ The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- ★ The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- ★ The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.
- ★ For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- ★ The customer's account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.
- ★ The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- ★ The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- ★ The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- ★ The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

- ★ The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds out of the account.
- ★ The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

13.2 Know Your Customer – The Basis for Recognising Suspicions

A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

Questions you must consider when determining whether an established customer's transaction might be suspicious are:

- ★ Is the size of the transaction consistent with the normal activities of the customer?
- ★ Is the transaction rational in the context of the customer's business or personal activities?
- ★ Has the pattern of transactions conducted by the customer changed?

13.3 Suspicious Scenarios

Issues which should lead you to have cause for suspicion would include:

- ★ Clients who are reluctant to provide proof of identity;
- ★ Clients who place undue reliance on an introducer (they may be hiding behind the introducer to avoid giving you a true picture of their identity or business);
- ★ Requests for cash related business, for example questions about whether investments can be made in cash, suggestions that funds might be available in cash for investment;
- ★ Where the source of funds for investment is unclear;
- ★ Where the magnitude of the available funds appears inconsistent with the client's other circumstances (i.e., the source of wealth is unclear). Examples might be students or young people with large amounts to invest;
- ★ Where the transaction doesn't appear rational in the context of the customer's business or personal activities. Particular care should be taken in this area if the client changes their method of dealing with you without reasonable explanation;
- ★ Where the pattern of transactions changes;
- ★ Where a client who is undertaking transactions that are international in nature does not appear to have any good reason to be conducting business with the countries involved (e.g., why do they hold monies in the particular country that the funds are going to or from? Do their circumstances suggest that it would be reasonable for them to hold funds in such countries?);
- ★ Clients who are unwilling to provide you with normal personal or financial information, for no apparent or rational reason. (Care should be taken not to include all distance relationships as suspicious, because most will be for genuine reasons. Suspicions will ordinarily be based upon cumulative as opposed to stand alone issues)

A money launderer is likely to provide persuasive arguments about the reasons for their transactions. Those should be questioned to decide whether a transaction is suspicious.

13.4 Reporting a Suspicion

Where, for whatever reason, we suspect that a client, or anybody for whom they are acting, may be undertaking (or attempting to undertake) a transaction involving the proceeds of any crime it must be reported as soon as practicably possible and in writing.

Internal reports must be made regardless of whether any business was, or is intended to be, actually written.

13.5 Investigation

Upon notification to the AML Compliance Committee an investigation will be commenced to determine if a report should be made to the appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file the SAR with the appropriate law enforcement or regulatory agency. The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agencies.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

13.6 Freezing of Accounts

Where we know that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen.

Do you have any questions?

If you are unsure of the things stated within this policy, or have any questions, please contact us either via our live chat features, which can be found on our website, or by emailing us at info@uexo.com.