AML and CFT Policy

Last updated: 06. 07. 2026

1. Policy statement

Metritax (MU) Ltd (the "Company", "we", "us") is incorporated in the Republic of Mauritius (registered number 235525 GBC) and licensed as an Investment Dealer (Full Service Dealer, excluding underwriting) by the Financial Services Commission of Mauritius (licence number GB26206169).

The Company is committed to maintaining effective measures to prevent money laundering, terrorist financing and proliferation financing. In pursuit of this objective, the Company complies with all applicable anti-money laundering and counter-financing requirements, including the Financial Intelligence and Anti-Money Laundering Act 2002 ("FIAMLA"), the Anti-Money Laundering Act 2026 ("AMLA"), the Financial Intelligence and Anti-Money Laundering Regulations 2018 ("FIAML Regulations 2018"), and applicable guidance issued by the Financial Services Commission ("FSC").
The Company's AML/CFT/CPF framework is designed in accordance with applicable laws, regulations and guidance issued by relevant authorities in Mauritius, including guidance issued by the Financial Services Commission and internationally recognised standards relating to the prevention of money laundering, terrorist financing and proliferation financing.

In line with these obligations and its internal policies, the Company performs due diligence on its clients. This includes verifying client identity, identifying beneficial owners, assessing the source of funds, analysing transactions, and monitoring for and reporting suspicious activity.

By accepting the Company's Customer Agreement, the client acknowledges that the Company may carry out these due diligence measures whenever necessary, without prior notice and without further consent. Where a complex due diligence process or an investigation is underway, activity on the client's account may be restricted.

This Policy applies to all officers, employees, and clients of the Company, and to every product and service the Company offers. All business units of the Company cooperate to maintain a coordinated defence against money laundering and terrorism financing.

The Company applies risk-based procedures reasonably designed to detect, prevent, and, where applicable, report suspicious transactions. All such efforts are documented and the records retained.

2. What money laundering and terrorism financing mean

2.1 Money laundering

Money laundering is the process of disguising the origin of money obtained through crime so that it appears to be legitimate income. It typically proceeds in three stages:

- **Placement** — the physical disposal of cash proceeds derived from criminal activity through, among other means, converting them into financial instruments or bank deposits in a manner that will not raise suspicions;
- **Layering** — moving the funds through a sequence of transactions designed to obscure their origin and break the audit trail.
- **Integration** — returning the "cleaned" funds to the economy so that they can be used without raising suspicion.

Money laundering covers a broad range of conduct designed to conceal the criminal origin of funds, including:

- acquiring, using, or possessing property derived from criminal activity;
- handling the proceeds of offences such as theft, fraud, or tax evasion;
- knowingly dealing with funds connected to criminal or terrorist activity;
- taking part in arrangements that facilitate the laundering of criminal or terrorist property;
- placing criminal proceeds into financial products;
- using criminal proceeds to acquire real estate or other assets; and
- moving criminal property within or across jurisdictions to evade detection.

Money laundering is not always a linear process. It may take the form of a single straightforward transaction, such as the purchase of a car or jewellery, or an elaborate structure of otherwise legitimate business operations built to conceal the true source of funds. Criminal property is not limited to cash: it may include rights, real estate, or other benefits. Knowing or suspecting that property derives from criminal activity, and failing to report it, itself amounts to participation in laundering.

No sector of the financial industry is immune to abuse by criminals. The Company therefore assesses the money laundering risks attached to its products and services and maintains robust controls to mitigate them.

2.2 Terrorism financing

Terrorism financing is the provision of funds or resources to terrorist activities or organisations, whether for ideological, political, or other motives, and the funds involved may come from entirely legitimate sources. Unlike money laundering, terrorism financing may not involve the proceeds of crime at all; instead, it seeks to conceal either the origin of funds or their intended future criminal use.

The Company must check that its clients are not themselves terrorists or terrorist organisations, and that they are not acting as a channel through which terrorist organisations are funded.

2.3 Proliferation Financing

Proliferation financing refers to the provision of funds, financial services or other forms of support that may contribute to the development, acquisition, manufacture, possession, transport or use of weapons of mass destruction and their related materials.

The Company recognises that proliferation financing presents a risk to the integrity of the international financial system and is committed to taking reasonable measures to identify, assess and mitigate such risks.

As part of its risk-based approach, the Company considers proliferation financing risks when conducting customer due diligence, screening customers and beneficial owners, monitoring business relationships and complying with applicable sanctions requirements.

The Company will not knowingly establish or maintain a business relationship with any person or entity that is subject to applicable sanctions or other restrictions relating to proliferation financing and will take appropriate action where concerns are identified.

3. Risk-based approach

The Company applies a risk-based approach: the depth of due diligence is proportionate to the risk presented by each business relationship. Scrutiny is intensified where the potential for money laundering is higher, so that effort is concentrated where it is most needed.

The Company assesses risk across four dimensions:
Client risk. Different client profiles carry different levels of risk. A baseline Know Your Client (KYC) check establishes the risk each client presents.

Product risk. A product or service presents higher risk where its characteristics could make it a useful tool for laundering. Such products attract heightened due diligence and closer monitoring.

Channel risk. How the Company onboards clients and delivers its services affects its exposure to money laundering and terrorism financing. Because the Company operates through non-face-to-face channels, it takes particular care to verify the documents it receives and to confirm the client's identity, so that the authenticity of those documents is assured.

Country risk. The client's geographic location, and the origin of the business activity, are risk factors in their own right: AML/CFT regulatory standards vary between jurisdictions, and those with weaker controls present a higher laundering risk. Enhanced due diligence is applied to clients and transactions connected to countries with elevated AML/CFT risk.

The Company regularly assesses the financial crime risks associated with its customers, products, services, delivery channels and the countries with which it conducts business. This helps ensure that resources and controls are focused on areas presenting a higher level of risk.

Evaluating these factors allows the Company to allocate its resources efficiently, direct enhanced due diligence at high-risk areas, and comply effectively with its AML obligations.

4. Procedures the Company implements to prevent money laundering and terrorism financing

The Company's AML/CFT framework rests on three principles: knowing its customers, monitoring their activity, and keeping appropriate records. To give effect to these principles, the Company implements the following procedures:

- identification and due diligence of clients, standard and enhanced;
- ongoing monitoring of business relationships and scrutiny of transactions;
- record-keeping in relation to clients' identity and their transactions;
- internal reporting of suspicious activity to the Compliance Officer (MLRO), and, where required, reporting to the competent authorities;
- refusal of suspicious transactions, rejection of third-party and anonymous payments, and freezing of accounts linked to criminal activity;
- internal controls and risk management directed at preventing money laundering; and
- measures to keep employees aware of these procedures and of the applicable AML/CFT legislation, supported by regular training in recognising and handling suspicious transactions.

Each procedure is set out below:

4.1 Client identification and due diligence (CDD)

As part of its due diligence process, the Company seeks to understand the purpose of the business relationship, the nature of the customer's activities and, where appropriate, the source of funds and source of wealth. The Company may also perform sanctions, politically exposed person (PEP) and adverse media screening as part of its customer due diligence measures.

Customer due diligence means identifying and verifying clients in order to assess their risk level and comply with AML/CFT regulations. The Company conducts CDD on every client before establishing a business relationship.

For identification, the Company collects the client's full name, date of birth, nationality, and residential address.

For verification, the Company requires:

- a national ID card, passport, or other government-issued identification document; and
- a utility bill, bank statement, or other document confirming the client's address, dated within the last three months.

For KYC purposes, the Company also collects information such as contact details, expected activity and volumes, and the source of funds. Information such as a tax identification number and country of tax residence may additionally be required for Common Reporting Standard purposes.

4.2 Enhanced due diligence (EDD)

The Company applies enhanced due diligence measures where a customer or business relationship presents a higher risk of money laundering, terrorist financing or proliferation financing.

Enhanced due diligence may be applied in circumstances involving politically exposed persons (PEPs), higher-risk jurisdictions, adverse media findings, complex ownership structures or any other situation where the Company determines that additional scrutiny is appropriate

The Company applies enhanced due diligence to higher-risk business relationships in order to mitigate money laundering and terrorism financing risk. EDD measures may include, without limitation:

- collecting additional information about the client's profile and the nature of the business relationship; and
- collecting and verifying additional information on the source of funds or source of wealth.

EDD may be triggered by, among other factors:

- the client being a Politically Exposed Person (PEP);
- adverse media reports concerning the client; or
- business activities that present an elevated risk of money laundering or terrorism financing.

Politically Exposed Persons. A PEP is an individual who holds, or has close ties to someone who holds, a prominent public position, for example, a Head of State or government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or important political party official. Because PEPs carry a heightened risk of corruption and improper influence, the Company applies additional measures to them, including enhanced due diligence.

High Risk Jurisdictions: The Company takes into consideration information issued by international organisations, regulators and competent authorities relating to jurisdictions that may present a higher risk of money laundering, terrorist financing or proliferation financing. Where appropriate, additional due diligence and monitoring measures may be applied.

4.3 Ongoing monitoring and transaction scrutiny

In accordance with the FIAML Regulations 2018, the Company monitors business relationships on an ongoing basis. This includes scrutinising transactions throughout the relationship, and, where necessary, confirming the source of funds, to ensure that activity remains consistent with the Company's knowledge of the client.

Particular attention is given to transactions that, by their nature, are vulnerable to money laundering, especially complex or unusually large transactions, and transactions with no apparent economic or lawful purpose.

The Company reviews customer information periodically and may request updated information or documentation where necessary to ensure that its records remain accurate and up to date. Additional reviews may be undertaken where there is a material change in the customer's circumstances or where unusual activity is identified.

4.4 Record-keeping

The Company retains all identification documents, transaction records, and risk assessment documentation for at least seven years after the business relationship with the client ends.

4.5 Internal controls, awareness, and training

The Company maintains internal control and risk management procedures directed at preventing money laundering and terrorism financing. Employees are made aware of these procedures and of the legislation relating to money laundering, and receive regular training to help them recognise and handle transactions suspected of being connected to money laundering or terrorism financing.

4.6 Suspicious transaction reporting

Suspicious activity, "red flags", may indicate money laundering or other unlawful conduct. Indicators include unusual transaction patterns, behaviour inconsistent with the client's profile, and connections to high-risk jurisdictions. Where suspicious activity is identified, further due diligence is carried out. If no reasonable explanation emerges, the activity must be reported to the MLRO/DMLRO, who is appointed to receive and assess all such internal reports.

Suspicious activity must be reported internally as soon as practicable. Internal reports must be made whether or not any business was transacted or intended. Where required, a suspicious activity report is submitted to the competent regulatory authorities.

Where the Company is unable to obtain sufficient information to complete its due diligence requirements, or where concerns arise regarding a customer or transaction, the Company may decline to establish or continue the business relationship and will consider whether the matter should be reported to the relevant authorities.

4.7 Refusal of transactions, payments, and freezing of accounts

The Company may refuse to process a transfer of funds at any stage if it believes the transfer is connected in any way to criminal activity or money laundering.

The Company does not accept third-party or anonymous payments. If the Company is not satisfied that the client is the sender of funds received, it may return those funds to the remitter, less any transfer fees or other charges, and may terminate the client's account.

The Company may freeze an account linked to criminal activity or fraudulent transactions, including where the account holder is suspected of involvement in such activity.

5. Sanctions and terrorist / proliferation financing

As a financial institution licensed in Mauritius, the Company complies with the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, which gives effect to United Nations Security Council measures aimed at maintaining international peace and security, including countering terrorism, terrorism financing, and the proliferation of weapons of mass destruction.

Such sanctions may include financial restrictions, arms embargoes, and travel bans in support of conflict resolution, nuclear non-proliferation, and counter-terrorism efforts.

The Company is also committed to identifying and managing proliferation financing risks and complying with applicable targeted financial sanctions. Appropriate screening and monitoring measures are implemented to help ensure compliance with these obligations

6. Review of this Policy

The Company may review and amend this Policy at its sole discretion, whenever it considers it appropriate to do so.