Anti-Money Laundering Policy

CONTENTS

1. TERMINOLOGY

Term used	Definition
'The company' or 'Insert'	Gilgamesh Financial Services and/or GFX Securities
'The Mauritius FSC'	The Mauritius Financial Services Commission
'The Mauritius FIU'	The Mauritius Financial Intelligence Unit
'The AMLCO'	The anti-money laundering compliance officer
'(The) regulations'	The responsibilities of Gilgamesh Financial Services and/or GFX Securities and/or the Company under regulations of Republic of Mauritius
'The Act'	I. Financial Services Act 2007; II. Code On The Prevention Of Money Laundering & Terrorist Financing 2012; III. Financial Intelligence and Anti-Money Laundering Act 2002; IV. Securities Act 2005; and V. The relevant acts, guidelines and regulations under the laws of Mauritius
'We', 'Us', 'Our', etc.	Management of Gilgamesh Financial Services and/or GFX Securities and/or the Company
'Relevant employee'	Any employee of Gilgamesh Financial Services and/or GFX Securities and/or the Company who might at any time possess information that will or should cause suspicion of money laundering
'Business relationship'	Is relationship is one that company enters into with a customer where both expect that the relationship will be ongoing
'Politically Exposed Persons (PEPs)'	means the natural persons who are or have been entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons
'Shell Bank'	means a credit institution or an institution engaged in equivalent activities incorporated in a jurisdiction which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group

2. INTRODUCTION

Five specific offences can be determined from the regulations, which apply generally to the employees of any company providing financial services or handling money in any capacity.

- Acquisition, use or possession of criminal property
- Acquiring, using or possessing criminal property is a criminal offence.
- Handling the proceeds of corruption
- Corruption by public sector employees or officials and politicians is a serious crime; handling the illicit results of this corruption is a criminal offence.
- Arrangements relating to criminal property

Any arrangement relating to criminal property, including but not limited to its permission or assistance in acquisition, retention or use, is a criminal offence. An employee of a company is permitted to defend themselves by proving that they reported their knowledge or suspicion of this immediately to the relevant authority in the correct manner.

'Tipping-off'

Revealing any information of any sort that could be considered by a reasonable person to affect an investigation into money laundering is a criminal offence.

Failure to report

Any person who knows of or suspects money laundering or otherwise could be considered to have reasonable grounds for knowledge or suspicion of the same commits a criminal offence by failing to report this to the competent authority or authorities.

It must be remembered that reporting knowledge or suspicion of money laundering is not under any circumstances considered to breach the requirements of financial companies to maintain their clients' confidentiality. Even if such knowledge or suspicion is not considered to be sustained under investigation, the only people who are informed of it are the reporter and the AMLCO, so a person incorrectly accused has their confidentiality maintained regardless.

3. GENERAL REQUIREMENTS

Under the regulations, the company has five main responsibilities in the area of AML compliance:

1. Appoint an AMLCO

   The AMLCO would be a senior employee with relevant experience at the company with authority to investigate all suspicions to the fullest. The AMLCO would be ultimately responsible for stressing to employees the consequences of failing to adhere to any of the requirements listed in this document.

2. Thoroughly check the identities of all new clients;
3. Simplify as much as reasonably possible for employees the process of reporting suspicious transactions;
4. Take and maintain complete records of clients' identities and transaction histories;
5. Educate and remind employees about the requirements in this booklet and how to raise suspicion.

4. KEY PEOPLE

The AMLCO

During the initial stages of the company's operations, the compliance officer will also assume the role of AMLCO. In this capacity, they will be ultimately responsible for implementing the regulations concerning AML. This means that in this document 'compliance officer' and 'AMLCO' refer to the same person; however, the specific tasks of each role are different. If in the future the management of the company sees fit to employ a separate person to act as AMLCO and take the associated responsibilities from the compliance officer, this document will be updated accordingly. As noted above, the AMLCO is a person of authority with access to any and all relevant information for the completion of their duties.

The AMLCO has four primary responsibilities:

1. Ensuring that employees are and remain aware of their responsibilities under the regulations;
2. Acting as a go-to person for relevant suspicions;
3. Forwarding/reporting all sustained suspicions to Mauritius FIU and Mauritius FSC;
4. Promptly responding to all communication from Mauritius FIU and Mauritius FSC.

The Annual Report of the AMLCO is a significant tool for assessing the company's level of compliance with its obligation laid down in the regulations.

The AMLCO's Annual Report shall be prepared and be submitted to the Board for approval within two months from the end of each calendar year (i.e. at latest, by the end of February each year).

The Annual Report deals with issues relating to money laundering and terrorist financing during the year under review and includes, inter alia, the following:

(a) information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the Directive which took place during the year under review

(b) information on the inspections and reviews performed by the AMLCO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the company applies for the prevention of Money Laundering and Terrorist Financing. In this respect, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation

(c) the number of Internal Suspicion Reports submitted by company personnel to the AMLCO;

(d) the number of reports submitted by the AMLCO to the Mauritius FIU and Mauritius FSC;

(e) information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues;

(f) summary figures, on an annualized basis, of clients' total deposit in Euro and other currencies in excess of the set limit of USD 10,000 (together with comparative figures for the previous year);

(g) information on the policy, measures, practices, procedures and controls applied by the company in relation to high-risk clients as well as the number and country of origin of high-risk clients with whom a business relationship is established or an occasional transaction has been executed;

(h) information on the systems and procedures applied by the company for the ongoing monitoring of client accounts and transactions;

(i) information on the measures taken for the compliance of branches and subsidiaries of the company, with the requirements of the regulations in relation to client identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements;

(j) information on the training courses/seminars attended by the AMLCO and any other educational material received;

(k) information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organized, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organization or consultants;

(l) results of the assessment of the adequacy and effectiveness of staff training;

(m) information on the recommended next year's training program;

(n) information on the structure and staffing of the department of the AMLCO as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against Money Laundering and Terrorist Financing.

The Compliance Officer

The compliance officer in turn has four primary responsibilities:

1. Updating the company's AML policies and updating these as might be required by the regulations;

2. Informing employees on how they might recognize suspicious transactions;
3. Ensuring full awareness as relevant of the policies in this document as well as the regulations among employees plus adherence to them;
4. Training new hires on the policies in this document and their duties to follow them as soon as practicable after onboarding.

5. STARTING RELATIONSHIP

Before the company can execute any transaction for any new client, a number of procedures need to be in place and carried out.

- AML procedures, namely identification, record-keeping, discovering and monitoring unusual or suspicious transactions and as appropriate internal reporting and control
- Employees know their responsibilities and the company's procedures
- Relevant training is being undertaken
- All relevant requests from outside sources are forwarded directly to the AMLCO

6. RISK BASED APPROACH

The company shall apply appropriate measures and procedures, by adopting a risk based approach, so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

Further, the AMLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Policy.

The adopted risk-based approach that is followed by the company, and described in the Policy, has the following general characteristics:

- recognises that the money laundering or terrorist financing threat varies across Clients, countries, services and financial instruments;
- allows the board of directors to differentiate between clients of the company in a way that matches the risk of their particular business;
- allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;

- helps to produce a more cost-effective system;
- Promotes the prioritisation of effort and actions of the company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the services of the company.

The risk-based approach adopted by the company, and described in the Policy, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the company.

Such measures include:

- identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular clients or types of clients, financial instruments, services, and geographical areas of operation of its clients;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- Continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators.

Such indicators include the following:

- The scale and complexity of the services offered;
- Geographical spread of the services and clients;
- The nature (e.g. non face-to-face) and economic profile of clients as well as of financial instruments and services offered;
- The distribution channels and practices of providing services;
- The volume and size of transactions;
- The degree of risk associated with each area of services;
- The country of origin and destination of clients' funds; deviations from the anticipated level of transactions; the nature of business transactions.

The AMLCO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the AMLCO shall also be responsible for the implementation of the policies, procedures and controls on a risk-based approach.

Principles of Risk Based Approach

The risk-based approach adopted by the company involves the identification, recording and evaluation of the risks that have to be managed.

The company shall assess and evaluate the risks it faces, for the use of the company's services for the purpose of Money Laundering or Terrorist Financing. The particular circumstances of the company determine suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the services and the financial instruments that the company provides are relatively simple, involving relatively few clients or clients with similar characteristics, then the company shall apply such procedures, which are able to focus on those clients who fall outside the 'norm'.

The company shall be, at all times, in a position to demonstrate to Mauritius FIU and Mauritius Financial Services Commission that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the company's services, for the purpose of Money Laundering and Terrorist Financing.

7. COMPANY RISKS

The following, inter alia, are sources of risks which the company faces with respect to Money Laundering and Terrorist Financing:

Risks based on the client's nature:

- complexity of ownership structure of legal persons;
- companies with bearer shares;
- companies incorporated in offshore centres;
- PEPs;
- clients engaged in transactions which involves significant amounts of cash;

- clients from high-risk countries or countries known for high level of corruption or organised crime or drug trafficking;
- Unwillingness of client to provide information on the beneficial owners of a legal person.

Risks based on the client's behaviour:

- client transactions where there is no apparent legal financial/commercial rationale;
- situations where the origin of wealth and/or source of funds cannot be easily verified;
- Unwillingness of clients to provide information on the beneficial owners of a legal person.

Risks based on the client's initial communication with the company:

- Non face-to-face clients;
- Clients introduced by a third person.

Risks based on the company's services and financial instruments:

- Services that allow payments to third persons/parties;
- Large cash deposits at banks to facilitate payments to the Company;
- Products or transactions which may favour anonymity.

8. RISK MITIGATION

Taking into consideration the assessed risks, the company shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost-effective manner. These measures and procedures include:

- Adaption of the client due diligence procedures in respect of clients in line with their assessed Money Laundering and Terrorist Financing risk;
- Requiring the quality and extent of required identification data for each type of client to be of a certain standard (e.g., documents from independent and reliable sources, third person information, documentary evidence);
- Obtaining additional data and information from the clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular business relationship or the occasional transaction;
- Ongoing monitoring of high-risk clients' transactions and activities, as and when applicable.

In this respect, it is the duty of the AMLCO to develop and constantly monitor and adjust the company's policies and procedures with respect to the client due diligence and identification procedures. These actions shall be duly documented and form part of the Annual Money Laundering Report, as applicable.

Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services and financial instruments provided by the company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the AMLCO to undertake regular reviews of the characteristics of existing clients, new clients, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

9. IDENTIFYING CLIENTS

Whenever the company receives supporting documents related to a new client's identity, it needs to be completely satisfied that they demonstrate the existence of the new client as a real natural or legal person and that they are indeed whom they say they are. Although the company will at times rely on third party sources as part of its fact-checking procedure when onboarding clients, the company bears ultimate legal responsibility for the checks being satisfactory.

Where the identification submitted is incomplete, inaccurate or otherwise insufficient, the company cannot proceed with opening an account for the client submitting such identification. Indeed, in more serious cases where money laundering, identity fraud or other crimes are suspected as opposed to simple carelessness or misunderstanding, the AMLCO would inform the Mauritius FSC.

The fact that no single identification can be completely guaranteed as genuine means that the company needs to use more than one document to confirm every new client's full name and address. As part of the company's policy of due diligence, five main pieces of information need to be collected and actions conducted:

- Establish the source of the applicant's funds
- Discover the applicant's net worth
- Find out the particular source of the funds to be deposited
- Where applicable, source references or any other appropriate documents that attest to the applicant's good reputation
- Conduct thorough background checks

The process is slightly different for individual clients and corporate clients, partially because the identities of companies and their reputations can be harder to establish conclusively.

10. INDIVIDUAL CLIENTS

Each individual applicant needs to present official identification containing their full name, nationality, date of birth and complete residential address. Documents accepted

are both of a passport, national ID or equivalent and a utility bill, bank statement, letter from government or reliable equivalent. Both of the documents submitted by each client need to be valid when they are submitted to the company.

11. CORPORATE CLIENTS

Institutional applicants listed on known stock exchanges or otherwise subjects of sound evidence that they are wholly owned subsidiaries or similar are not subject to any extra checks beyond those customary checks in other cases.

Other companies however do need to have their existence, standing and identity confirmed as well as the authority of the people acting for them verified. The documentation required for this can differ from country to country and between companies, but under most circumstances they would be some or all of these:

- Incorporation certificate or similar
- Incumbency document or equivalent (this needs to state the applicant company's current directors clearly)
- Statutes, articles of association or other analogous documents proving that the natural person applying has permission to enter the applicant company into a legal agreement
- If necessary and available, an extract from the commercial register of the applicant company's country of incorporation would be requested to support the other documents

AMLCO and his associates must understand the structure, the beneficial owners and all of the officers of the institutional client before accepting such a client.

Beneficial owners

KYC and due diligence on owners of accounts also differs from individual clients to institutional clients.

For individuals, the company needs to be sure from the documents etc submitted that the client applying is acting on their own behalf and not on behalf of another natural or legal person.

For institutional clients, the company needs to know the applicant company's structure from the documents submitted. It also needs to know where the funds for the account would come from, who are the main owners (or singular owner) of the company's stock if this applies in addition to verifying the identities of the company's board of directors or equivalent (i.e. who has ultimate control over the applicant company's money). In all cases, the AMLCO would make a reasonable informed judgement on whether further information is required.

12. PEPs

The Company shall apply the following with respect to the accounts of "Politically Exposed Persons":

1. The establishment of a Business Relationship or the execution of an occasional transaction with persons holding important public positions and with natural persons closely related to them, may expose the Company to enhanced risks, especially if the potential Client seeking to establish a Business Relationship or the execution of an Occasional Transaction is a PEP, a member of his immediate family or a close associate that is known to be associated with a PEP.
2. The general policy of the Company is not to deal with PEPs.

13. METHODS OF SUBMISSION

Clear scans of documents sent by email or through the company's CRM are normally acceptable. Sometimes though the company might need to see certified copies or originals. Documents could be certified by a notary public or other similar authority, an appropriate public sector official or an authorised financial institution. Copies of documents can also be certified by employees of the company if they are made in employees' presence.

If any document relevant to a corporate entity (such as extract from a register of commerce) is available online through a relevant official website, the company may refer to the online version of the document on condition that a printout is made by an employee of the company and stored in the appropriate client's file.

In addition to these documents, clients need to provide their phone numbers and email addresses.

14. HIGH RISK

Various countries have been identified by the FATF in the so-called 'FATF blacklist' as having insufficient AML standards. Applicants from these countries are subject to at the minimum higher scrutiny, and applications from residents of countries under the category 'call to apply counter-measures' would not be accepted.

The risks of applicants from offshore jurisdictions are on the whole covered by the measures outlined in this document; however, the transactions of such clients were they to be accepted would be subject to elevated scrutiny by the company. This also applies to clients whose wealth is known to come from activities vulnerable to money laundering.

15. ONGOING DUE DILIGENCE

The constant monitoring of the clients' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing.

In this respect, the AMLCO shall be responsible for maintaining as well as developing the on-going monitoring process of the company. The Internal Auditor (once appointed) shall review the company's procedures with respect to the on-going monitoring process, at least annually.

The procedures and intensity of monitoring clients' accounts and examining transactions on the client's level of risk shall include the following:

1. The identification of:

- transactions which, as of their nature, may be associated with money laundering or terrorist financing;
- unusual or suspicious transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation;
- In case of any unusual or suspicious transactions, the relevant employee shall be responsible to communicate with the AMLCO.

2. Further to point (a) above, the investigation of unusual or suspicious transactions by the AMLCO. The results of the investigations are recorded in a separate memo and kept in the file of the clients concerned;

3. The ascertainment of the source and origin of the funds credited to accounts;

4. The use of appropriate IT systems

16. VERIFICATION AND RECORD KEEPING

Responsibility for verifying applicants' identities rests with the AMLCO. Verification must be complete with sufficient evidence before any customer agreement can be sent to an applicant.

The procedure followed for establishing every applicant's identity is recorded along with a copy of the client's completed identification questionnaire. If at any stage back office staff are unsure which information is required for an identity to be checked, the AMLCO must be consulted before proceeding.

Completed client identification questionnaires should be signed by the employee processing them and stored by the compliance officer after being countersigned by the latter. At this stage the compliance officer also decides whether additional information is required before an applicant is permitted to hold an active account. All records taken in this way by the compliance officer plus records of clients' orders are kept for a minimum of five years.

17. TRAINING

Every employee in back office needs to know about AML laws and regulations, who the AMLCO is and what their role is, what the role of the back-office team is to apply the procedures in this document and the possible results of any breaches in AML compliance.

All employees will receive regular training on these matters and be required to revise this document regularly. Training might include seminars organized by the compliance function, computerized questions testing knowledge at regular intervals and informal discussions. Records of these are to be kept; such documentation would include who attended which types of training and when plus details of what was discussed.

18. DUTY TO REPORT

Any employee who suspects money laundering needs to report it. Beyond this, though, if reasonable grounds are deemed to exist for suspicion of the same, an employee would be committing an offence by not suspecting and reporting. This is why clear and strong KYC policies are essential for preventing money laundering and related activities and it is also essential that employees share the company's commitment to these.

'Knowledge of money laundering' can of course vary in its definition, but a reasonable person might concur that it could include intentional ignorance of what should be suspicious to an honest person and failure to ask the questions which would be appropriate to a reasonable person.

Suspicion can also be defined in different ways but it does need to be something beyond vague conjecture. An objective test for reasonable grounds for suspicion then could include the factors above in addition to a failure to analyse and evaluate sufficiently the information available.

Preventing ambiguity in the definitions of 'knowledge' and 'suspicions' necessitates that the company make as certain as it can that its staff fully understand these KYC policies in their entirety.

19. INTERNAL REPORTING

As above, employees must report any relevant suspicion to the AMLCO. All suspicions must be detailed in full with names of everyone involved, full information on the client's account and as complete as possible a description of what gave rise to the suspicion. Any internal enquiry about a report also needs to be documented.

After submission, the AMLCO should remind the reporting employee to avoid 'tipping-off' the subject and that any information submitted must not be disclosed to anyone except the AMLCO. Note that an employee still needs to report even when a transaction has not been completed because of suspected money laundering. Whenever a report is received, the ALMCO considers its contents. If the suspicion is sustained after this analysis by the AMLCO, the report is forwarded to Mauritius FSC: this process does not need to be and should not be approved by anyone other than the AMLCO.

When considering reports, the AMLCO will study any information and documentation necessary, particularly KYC documents as listed earlier in this policy document.

20. SUSPICIOUS TRANSACTIONS

'Suspicious transaction' might reasonably be defined as a transaction incongruent with a particular client's profile and/or known legitimate business activities. This is why KYC is so important.

The following list of commonly used questions can help to determine whether a transaction could be suspicious:

- Does it broadly make sense for this client?
- Is its size relative to the client's profile abnormal in any way?
- Is it unusual considering the client's historic transactions?
- Are there any suspicious transactions linked with it?
- Is the manner of payment suggested by the client in any way odd?
- Does it together with others demonstrate a significant change to the usual pattern of this client's transactions?

Any suspicion of money laundering, however seemingly unimportant to the employee who might have it, needs to be raised as soon as possible with the AMLCO using the internal reporting form included at the end of this document. Every credible or sustained report received in this way must be forwarded to the Mauritius FSC by the AMLCO.

21. INTERNAL REPORTING FORM

Part 1: involved parties

Individual	**Name**	*Insert name of individual*
	Date of birth	*Insert date of birth*
	Address	*Insert address*
	Contact details	*Insert any contact telephone number or email address*
	Additional details	*Insert any further details that may be known about the individual*
	Involvement	*This should indicate the involvement as you understand it of this party in the activity you are reporting, eg client of the firm*

Other party	**Name**	*Insert name*
	Address	*Insert address*
	Contact details	*Insert any contact telephone number or email address*
	Additional details	*Insert any further details that may be known (for example, any company numbers or websites)*
	Involvement	*This should indicate the involvement as you understand it of this party in the activity you are reporting, e.g. victim*

You should create as many tables as required for your case and complete as much information as known for each party.

Part 2: reason for suspicion

Guidance on completing this section

Provide a summary to explain your suspicion and then provide a chronological sequence of events. Try to keep the content clear, concise and simple. For

Example, explain how you became aware of the situation, describe the events, activities and/or transactions that led you to be suspicious, and how and why you became suspicious because of these.

As a guide when submitting a Report, wherever you can, try to answer the following six basic questions to make the information provided as useful as possible:

- *Who?*
- *What?*
- *Where?*
- *When?*
- *Why?*
- *How?*

Remember to include:

- *the date of activity*
- *the type of product or service*
- *how the activity will, or has, taken*

If you are suspicious because the activity deviates from the normal activity for that individual/firm, briefly explain how the activity that gave rise to your suspicion differs from the normal.

***TIP/REMINDER** Have you clearly described the suspicion? This report will be read by a third party and potentially forms a basis of a report to Law Enforcement/ Authorities. Have you clearly explained your concern so a third party can understand?*

Part 3: supporting documentation

Attach any supporting documentation that is relevant for the case. For example, this may include copies of correspondence, customer files or information that you have obtained on the matter. *For each file attached, ensure that an explanation is provided of what it is, as this will help the third party when reviewing the case.*

Part 4: submitter's details

Name	
Contact number	
Date of report	

22. CONFIDENTIALITY

A watertight defence against a claim for breach of confidence is reporting a suspicion of money laundering. Nonetheless, comments to any third parties such as the press of any sort need to be made through the AMLCO, as should any information requested from them. This is to prevent the offence of 'tipping-off'.

23. INTERNAL AUDITOR

The following obligations of the Internal Auditor are addressed specifically for the prevention of Money Laundering and Terrorist Financing:

(a) the Internal Auditor shall review and evaluate, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of Money Laundering and Terrorist Financing mentioned in the document;

24. EXTERNAL REPORTING

Any suspicion of a client or an activity that is sustained will be reported to the Mauritius FIU and Mauritius FSC. This would normally be by means of a forwarded internal report. If the regulator then requires more details, the company would make certain that all relevant information is sent to the Mauritius FSC without delay.