



# GECOBITEXCHANGE

## AML POLICY

Role(s)	Summary of responsibilities
Money Laundering Compliance Officer (MLCO)	<ul style="list-style-type: none"> <li>● sufficiently senior employee, with sufficient skills, experience and knowledge in AML/CTF and Compliance</li> <li>● ensuring and reviewing the efficacy of this policy</li> <li>● ensuring there are mechanisms to facilitate the reporting of any suspicions that money laundering may be taking place, receiving and investigating any such reports and in turn making reports to the NCA</li> <li>● ensuring arrangements are in place to store and retain due diligence and other AML documentation</li> <li>● ensuring the company's compliance with all applicable laws</li> <li>● protecting the company from the risks associated with breaches of the law</li> <li>● preserving the good name of the company against the risk of reputational damage presented by implication in money laundering and terrorist financing activities</li> <li>● making a positive contribution to the fight against crime and terrorism</li> </ul>

## POLICY STATEMENT

Company aim, by having robust policies and procedures and the creation of an internal compliance culture, is to prevent money laundering and terrorist financing.

In order to achieve this, we have undertaken the following:

- based on business nature and requirements we have established appropriate and risk-sensitive policies and procedures relating to:
  - customer due diligence
  - reporting
  - record-keeping
  - internal control
  - risk assessment and management
  - compliance management
  - communication
- the following training policy was declared to ensure at least MLCO is self-trained at regular intervals for:
  - awareness of the relevant legislation and any changes
  - updates on particular threats and alerts for the company
  - updates on knowledge how to recognize potential suspicious activity
  - how to report suspicious activity
  - the company's exposure to risk
  - the company's client due diligence policies and procedures
- company will retain the following records for five years after ceasing to act for a client:
  - client's risk assessments
  - client 's identity and verification
  - client's ongoing monitoring
  - internal reporting
  - external reporting
- company through the MLCO has established automated procedures for assessing internal suspicious activity reports and on the decision-making process for external reporting
- company have established procedures for making suspicious activity reports to the NCA and for the secure retention and storage of internal and external reports
- company through the MLCO has established procedures for aiding any law enforcement agencies who obtain money laundering investigation orders against our clients
- company develops software to automate daily tasks, make them accurate, mitigate risk related to employee involvement in business daily processes



- company staff is aware of the guides and does refresh knowledge when needed from the following website <https://www.politsei.ee/et/juhendid>



- before starting any business with the client, screening for sanctions, PEP status is done via automated or manual processes
- company sets a daily transaction limit in amount of 14 999 EUR for all clients
- based on <https://www.riigiteataja.ee/en/eli/511122019005> company must identify a person and verify data with the help of information technology means where a business relationship is established with a person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country and whose total sum of outgoing payments relating to a transaction or a service contract exceeds 15 000 euros per calendar month or, in the case of a customer who is a legal person, 25 000 euros per calendar month, and where the due diligence measures are not applied while being physically in the same place as the person or their representative
- client contact details are verified at least on a yearly basis
- company never uses cash in business operations with the client
- changes will be made to the AML policies and procedures of the business when appropriate to ensure compliance

## CUSTOMER DUE DILIGENCE

The business has established KYC policy to ensure that the identities of all new and existing clients are verified to a reasonable level of certainty. Based on nature of the services provided this will include individual and business entities (clients). Clients will be verified online (using information technology means) - manually by MLCO or with the help of only recognized online identity verification agencies (list of such is added in the end of this document with MLCO comments). Person from a country outside the European Economic Area should be identified face-to-face while being physically in the same place. Company must apply CDD measures before entering into a business relationship or carrying out an occasional transaction. CDD procedures should be applied not only to all new clients but also to existing clients at appropriate times.

The following documentation should be presented by the individual or business entity owner/director:

- either a passport, driver's license, or government issued document featuring a matching photograph of the individual, and a full name and date of birth matching those provided
- original recent utility bill, or government issued document with the same address matching those provided by the individual
- for business entities as an extra measure mining proof documents might be required (electricity bills, mining equipment purchase proof documents etc)

If the business fails to verify the identity of a client with reasonable certainty it will not establish a business relationship or proceed with the transaction. If a potential or existing client either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the business shall refuse to commence a business relationship or proceed with the transaction requested.

The purpose of CDD is to ensure that company knows who is client and can trust that client is using company's services for legitimate reasons. Risk-based approach will be taken and low risk client will go through completely automated workflow and for medium to high risk client's workflow is switched to manual review by MLCO.

Good knowledge of a client's business and financial background as well as information on the purpose and intended nature of the business relationship is also very important in order to provide an effective service, to the client.

Additionally, company should be alert and corroborate accordingly, on the reasons why any of their existing and/or potential clients is changing professional service providers. Frequent and unjustifiable changes in professional service providers may be a red flag.

For individuals at least following information is required:

- full name
- personal code
- government issued document (name of the document, number, issue date, expire date)

- living address
- source of funds, marital status
- contact details like phone number and email address

For business entities at least the following information is required:

- Verify the beneficial owner identity and place of residence
- Take steps to understand the ownership and control structure of the client
- Get registration and incorporation documents
- Assess the purpose of the intended nature of business relationship
- Get additional supporting documents (recent bank statement, Utility bills e.g. electricity)

CDD measures will be carried out:

- when establishing a business relationship
- when carrying out an occasional transaction
- where there is a suspicion of money laundering or terrorist financing
- where there are doubts concerning the veracity of previous identification information

CDD procedures should be applied not only to all new clients but also to existing clients at appropriate times. More specifically for existing clients, CDD procedures may be performed when the relevant circumstances of the client change or during scheduled/routine CDD updates. Change-driven updates of the CDD may be triggered by:

- Suspicions
- Changes in the client BO
- Changes in services provided
- Changes in professionals servicing the client
- Changes in general affairs
- Changes in line of business
- Changes in geographical area of operations
- Changes in key management
- Any other changes

Scheduled/routine CDD updates should be carried out on a risk sensitive basis. Hence the higher the risk the more frequent the scheduled CDD update should be carried out.



CDD measures are applied to all clients, both at the start of an engagement and then on an ongoing basis. When establishing a business relationship, company does identify and verify the client's identity using documents, data or information from reliable and independent sources.

Company will assess the money laundering risk represented by our clients and the business conducted according to three levels:

- negligible(low) level of risk requiring only SCDD (automated by developed software)
- medium/normal level of CDD (manual by MLCO)
- exceptionally high level of risk requiring an ELCDD (manual by MLCO)

Person with PEP status, or family relation to PEP is automatically set to HIGH RISK and requires ELCDD and in most of the cases should not start any business with the company.

LOW category clients:

- Estonia resident
- EU resident
- UK resident
- Estonia companies
- EU companies

MEDIUM category clients:

- Russia and post-Soviet country residents
- Russia and post-Soviet country companies

HIGH category clients:

- PEP or with relation to PEP (family etc)
- US resident

Company will identify and maintain lists of risk factors relating to clients, products or services, transactions, delivery channels and geographic areas of operation.

Company will update the risk assessment annually to ensure new and emerging risks are addressed, and new information supplied is reflected.

PEP can be identified by:

- asking directly upon registration process
- searching through PEPs databases
- search through media sources

PEP individuals are subject for manual review and MLCO decision to start business relationship or not.





## ASSESSMENT OF MONEY LAUNDERING RISK

It is the policy of this company to verify the identity of all clients, ensuring that procedures reflect client risk characteristics. It is the policy of this company to check that clients are not the subject of sanctions or other statutory measures prohibiting the company from providing its services.

Company is taking a risk-based approach in monitoring the financial activities of its clients. This will be carried out business with the client.

Company will actively not accept high-risk clients that are identified as follows:

- clients with larger one-off transactions, or a number of transactions carried out by the same customer within a short space of time
- unusual patterns of transactions that have no apparent economic or visible lawful purpose
- money sent to or received from areas known to have high levels of criminality or terrorist activity

Company will conduct ongoing monitoring of business relationships with customers, to ensure that the documents, date or information held evidencing the customer's identity are kept up to date.

The following are examples of changes in a client's situation that may be considered suspicious:

- sudden increase in business from an existing customer
- uncharacteristic transactions which are not in keeping with the customer's known activities
- peaks of activity at particular locations or at particular times
- unfamiliar or untypical types of customer or transaction

Whenever there is cause for suspicion, the client will be asked to identify and verify the source or destination of the transactions, whether they be individuals or company beneficial owners.

No action need be taken if there is no cause for suspicion.

In order to evaluate the severity of a risk, company first want to know the impact of that risk if it occurs, and the likelihood of it occurring.

Company have developed categories of impact as follows:

Limited	Minor	Moderate	Major	Catastrophic
1	2	3	4	5

Each category of impact is accompanied by a score.

	Limited	Minor	Moderate	Major	Catastrophic
Value of transaction	Very limited value				Max daily limits funds systematically laundered
Reputation	No impact on reputation				Business fails as a result of publicity
Reach	Isolated to your company				Systemic abuse of the regulated sector (lawyers, banks etc)
Resources	Minimum resources required to address the risk				Required resources exceed company's abilities

Company uses the following process in measuring the likelihood:

	Rare	Unlikely	Possible	Probable	Highly probable
Measure of occurrence	<5%	6-20%	21-40%	41-60%	>60%
Score	1	2	3	4	5

The overall risk score is calculated using the following formula:

$$\text{Likelihood} \times \text{Impact}^2$$

Scores to identify the overall level of risk:

5-HIGHLY PROBABLE	5	20	45	80	125
4-PROBABLE	4	16	36	64	100
3-POSSIBLE	3	12	27	48	75
2- UNLIKELY	2	8	18	32	50
1- RARE	1	4	9	16	25
	1- Limited	2- Minor	3- Moderate	4- Major	5- Catastrophic

Each score is categorized with a color. The color that your risk score comes out at translates into a response to that risk as follows:

	Risk outcome	Response required
<b>RED</b>	HIGH Score of above 50	Take urgent action to manage the risk
<b>AMBER</b>	MEDIUM/HIGH Score 20-49	Take action to manage the risk
<b>YELLOW</b>	MEDIUM/LOW Score 5-19	Monitor this risk
<b>GREEN</b>	LOW Score 1-4	Tolerate this risk

Company assess clients by comparing their characteristics and transactions with those listed in the risk register. This will promote consistency of treatment of clients throughout client base. Company will assess clients and record such assessment but this does not have to be very detailed or difficult.

Automatic HIGH risk:

- document verification ends with falsification result
- client can't explain the source of funds
- client who is under local AML investigation wants to do transaction in amount of daily limit
- client is asking/searching for replacement of transaction with cash withdrawal

All verification of identity processes will be recorded. This will include keeping photocopies of documents produced, or in exceptional cases with the approval of the MLCO, recording information about where copies are held and can be obtained.

## Lower risk

### **Non-exhaustive list of factors and types of evidence of potentially lower risk:**

#### **1. Customer risk factors:**

- (a) Public companies listed on a stock exchange and subject to disclosure requirements, either by stock exchange rules or through law or enforceable means, which impose requirements to ensure adequate transparency of beneficial ownership
- (b) public administrations or enterprises
- (c) customers that are resident in geographical areas of lower risk

#### **2. Product, service, transaction or delivery channel risk factors:**

- (a) life insurance policies for which the premium is low
- (b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral
- (c) a pension or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme
- (d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes
- (e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership such as certain types of electronic money

#### **3. Geographical risk factors:**

- (a) Member States of the European Union
- (b) third countries having effective AML/CFT systems
- (c) third countries identified by credible sources as having a low level of corruption or other criminal activity
- (d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements

## Higher risk

### **Non-exhaustive list of factors and types of evidence of potentially higher risk:**

#### **1. Customer risk factors:**

- (a) the business relationship is conducted in unusual circumstances
- (b) customers that are resident in geographical areas of higher risk as set out in paragraph
- (c) legal persons or arrangements that are personal asset-holding vehicles
- (d) companies that have nominee shareholders or shares in bearer form
- (e) businesses that are cash-intensive
- (f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business

#### **2. Product, service, transaction or delivery channel risk factors:**

- (a) private banking
- (b) products or transactions that might favor anonymity
- (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures
- (d) payment received from unknown or unassociated third parties
- (e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products

#### **3. Geographical risk factors:**

- (a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems
- (b) countries identified by credible sources as having significant levels of corruption or other criminal activity
- (c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations
- (d) countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country

**Risk Factors as highlighted by FATF:**

- The client's and the client's beneficial owner's business or professional activity, i.e. whether the activity carries a high risk of corruption (e.g. arms dealing), whether it relates to high levels of cash, whether they are regulated, etc.
- The client's and the client's beneficial owner's reputation i.e. are there adverse media surrounding the client and the beneficial owners, are they subject to previous suspicion report or have they been convicted, etc.
- The client's and the client's beneficial owner's nature and behavior i.e. are they unnecessarily secretive, is their doubt of the veracity of the KYC documents, is there frequent and inexplicable change in ownership, etc.
- The client's structure, i.e. is the structure non-transparent, unusually complex with no reasonable explanation, etc.
- Individuals subject to sanctions issued by the U.N., EU and OFAC.
- The level of transparency the service/transaction affords, i.e. do these services promote anonymity, do firms accept instructions given by a third party, etc.
- The complexity of the service/transaction, i.e. whether the transactions involve a number of parties from a number of jurisdictions.
- The value or size of the service/transaction, i.e. whether the services cash intensive or involve high value transactions.
- Countries not having adequate AML/CTF systems e.g. FATF and EU high-risk third country lists.
- Countries subject to sanctions, embargoes or similar measures issued by, for example the U.N., EU and OFAC.
- Countries having significant levels of corruption or other criminal activities such as narcotics, arm dealing, human trafficking, illicit diamond trading, etc.
- Countries identified to support terrorist activities, or have designated terrorist organizations operating within their country.
- The channels through which the Licensed Firm establishes a business relationship or through which transactions are carried out. Channels that favor anonymity increase the risk of ML/TF if no measures are taken towards this.
- In the cases where interaction with the client takes place on a non-face to face basis, technological measures can be put in place to mitigate the heightened risk of identity fraud or impersonation present in these situations. These measures allow a Licensed Firm to establish whether the client providing the relative identification details is actually the person he alleges to be.

**Money Laundering red flags Examples of suspicious transactions/ activities related to money laundering:**

- Transfer of funds between bank accounts established in various countries, without justified reason.
- Transfer of funds between companies belonging to the same group, without justified reason.
- Deposits performed without submission of supporting documentation in an accepted form (e.g. invoice, agreements etc.).
- Supporting documentation that is submitted in relation to a specific transaction (e.g. an invoice or agreement) is not in the same form that is normally used by the client. For example, draft invoices, different from those produced from the system used by the client are submitted.
- Transactions with no apparent purpose or which are unnecessarily complex.
- Use of foreign bank accounts or companies or groups of companies with a complicated ownership structure which is not justified based on the needs and economic profile of the client.
- The transactions or the size of the transactions requested by the client do not comply with the client's usual practice or business activity.
- Large volume of transactions and/or money deposited or credited into an account, when the nature of the client's business activities would not appear to justify such activity.
- Frequent settlement of client's obligations in cash.
- Use of bank accounts other than the client's usual bank accounts, to transfer amounts initially deposited in cash.
- Any transaction of which the nature, size or frequency appears to be unusual.
- Instructions of payment to a third person that does not seem to be related with the instructor.
- Transfer of funds to and from countries or geographical areas which do not apply or inadequately apply the FATF Recommendations.
- A client is reluctant to provide complete information when establishing a business relationship about the nature and purpose of the client's business activities, anticipated account activity, names of officers and directors, or business location.
- A client is providing minimum or misleading information that is difficult or expensive for the firm to verify.
- A client provides unusual or suspicious identification documents.
- A client's home/business telephone is disconnected and the client cannot be reached by the firm and its employees.
- A client who has been introduced by a foreign financial organization, or by a third party from countries or geographical areas which do not apply or inadequately apply the FATF Recommendations.



- Financial transactions from non-profit or charitable organizations for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Unexplained inconsistencies arising during the process of identifying and verifying the client.
- Complex trust or nominee network and/or legal structure.



**Terrorist Financing red flags Examples of suspicious transactions/activities related to terrorist financing:**

- A series of complicated transfers of funds from one legal or physical person to another as a means to hide the source and intended use of the funds.
- Transactions which are inconsistent and are not economically justified considering the organization's normal activity.
- Deposits are structured below the reporting requirements to avoid detection.
- Multiple cash deposits and withdrawals with suspicious references.
- Frequent domestic and international ATM activity.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected. Unusual cash activity in foreign bank accounts.
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- Use of multiple, foreign bank accounts.
- Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.
- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- Wire transfers to areas of conflict.
- Financial activity identifiable with travel (e.g. purchase of airline tickets) to jurisdictions adjacent to areas of conflict.
- Sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.
- The parties involved in transactions (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- Use of false corporations, including shell-companies.
- Existence of media reports referring to account holder who are linked to known terrorist organizations or is engaged in terrorist activities.

## VERIFICATION OF CLIENT'S IDENTITY (KYC)

KYC information in all cases, even where clients qualify for simplified due diligence under the terms of the Money Laundering Regulations, or where they are considered low risk for other reasons, to assist in effective ongoing monitoring, company still should gather knowledge about the client to allow understanding of:

- who the client is?
- purpose and intended nature of the business relationship
- nature of the client
- client's source of funds
- client's status and economic purpose

The above points are a part of the 'know your client' information. Good KYC information may be used where the accumulation of the knowledge may be sufficient to prove the identity of a client without requiring some of the additional documents, data or information under the enhanced due diligence procedures. The length of time the client has been known and depth of knowledge of his circumstances are good elements under KYC helping to reduce risk to one that is normal or lower.

In practice the following questions would be suitable

- full name (forename, middle, surname and title)
- current address
- how long have you lived there?
- what is your previous address (if under 12 months)
- date of birth
- marital status (e.g. married, divorced, widowed)
- nature of the business relationship
- nature, type and geographical locations of the client and its interests
- previous/current employments

We are specifically required on a risk sensitive basis to find out if we have a PEP as a potential client. Our guidance notes also require us on a risk sensitive basis to ensure we are not dealing with individuals on the Sanctions listings.

Clients who are politically exposed persons must always be subject to enhanced due diligence measures including enhanced ongoing monitoring. Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position makes them vulnerable to corruption. This risk also extends to members of their immediate families and to know close associates. PEP status itself does not, of course, incriminate individuals or entities. It may, however, put a customer into a higher risk category. Although under the definition of a PEP an individual cease to be so regarded after he has left office for one year. In many cases, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated. Public functions exercised at levels lower than national should normally not be considered prominent.

However, when their political exposure is comparable to that of similar positions at national level, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Prominent public functions include:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliaments
- members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, charges d'affaires and high-ranking officers in the armed forces; and
- (other than in respect of relevant positions at community and international level)
- members of the administrative, management or supervisory boards of state-owned enterprises

Persons known to be close associates include:

- any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP
- any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP. For the purpose of deciding whether a person is a known close associate of a PEP, the firm must have regard to any information which is in its possession, or which is publicly known.
- having to obtain knowledge of such a relationship does not presuppose an active research by the firm.



The additional check may consist of robust anti-fraud checks that the company routinely undertakes as part of its existing procedures, or may include:

- requiring the first payment to be carried out through an account in the customer's name with EU regulated credit institution or one from an equivalent jurisdiction
- withdrawals are done only to an account in the customer's name with EU regulated credit institution
- verifying additional aspects of the customer's identity, or of his electronic 'footprint'
- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration)
- internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address
- other card or account activation procedures
- requiring copy documents to be certified by an appropriate person



## ONGOING MONITORING OF CLIENTS' ACTIVITIES

The MLCO will regularly monitor the following procedures to ensure they are being carried out in accordance with the AML policies and procedures of the business:

- client identity verification
- reporting suspicious transactions
- record keeping

### POLICY

It is the policy of this company to monitor clients' instructions and transactions to ensure consistency with those anticipated and with the client risk profile. Instructions and transactions will be monitored to ensure that possible grounds to suspect money laundering will be noticed and scrutinized, and changes requiring a re-assessment of money laundering risk will be acted upon.

### CONTROLS AND PROCEDURES

- MLCO will maintain alertness for clients' instructions and transactions which represent a significant divergence from those anticipated for the client
- an automated transaction monitoring system is to be used, it will be developed in house and risk assessed prior to use
- where a client's instruction or transaction is not consistent with what is anticipated:
  - an explanation will be sought, if appropriate by contacting the client
  - involvement of unexpected jurisdictions or organizations will be checked with the company's MLCO for possible alerts or sanctions
  - if a satisfactory explanation is found, the client file will be updated to record that explanation and to reflect the change in anticipated client activities
  - if no satisfactory explanation is found, MLCO will consider whether there are grounds to suspect money laundering
  - MLCO will consider whether there is cause to carry out a re-assessment of money laundering risk, and if so, will carry this out
  - irrespective of whether specific incidents have caused a re-assessment of money laundering risk, every client file will be reviewed periodically to check that:
    - information held is still adequate, correct and up to date
    - level of client due diligence being applied is still appropriate
- periodic review of client files will be conducted at the following intervals:
  - for high-risk clients – every three months
  - for all clients – every six months
- periodic review of client files for AML due diligence purposes can be conducted at the same time as business development reviews, but the AML review must be separately noted on the file

## KEEPING RECORDS

It is the policy of this company to establish and maintain systems to keep records of enquiries made and information obtained while exercising CDD for AML purposes, and to ensure that these records are retrievable as required for legal and regulatory stipulations. These records will include but not be limited to details recorded for accounting and business development purposes.

## CONTROLS AND PROCEDURES

- when information is being collected for AML CDD, the responsible MLCO will ensure that:
  - information collected is recorded in a consistent manner in the client file, or other appropriate place, and that CDD records held in different places are cross referenced where appropriate, so that CDD information is accessible by MLCO
  - all instances are recorded where information requested has not been forthcoming, or explanations provided have not been satisfactory
- company will have systems to routinely archive CDD records along with the company's accounting records to ensure their availability for a minimum of five years from the date of the completion of the transaction or enquiry
- company will have data retrieval systems which facilitate full and rapid retrieval of all relevant CDD records by authorized staff, in order to respond fully to enquiries from financial investigators
- company will have procedures to ensure that any personal data obtained for CDD purposes is processed only for the purposes of preventing money laundering and terrorist financing
- for clients who have been the subject of a suspicion report, relevant records will be retained separately from the company's routine archives, and not destroyed, even after the five-year period has elapsed, without confirmation from the MLCO that they are no longer required as part of an enquiry

The records that company is going to keep:

- copy of, or the references to, the evidence of the customer's identity obtained under the customer due diligence requirements in the regulations
- supporting evidence and records in respect of the business relationships and occasional transactions which are the subject of customer due diligence measures or ongoing monitoring
- copy of the identification documents accepted and verification evidence obtained
- references to the evidence of customer's identity
- transaction and business relationship records (account files, relevant business correspondence, including electronic mail, daily logs, receipts, etc.)

Evidence of customer's identity records will be kept for five years beginning on the date on which the occasional transaction is completed or the business relationship ends. Records of transactions (whether undertaken as occasional transactions or part of a business relationship) will be kept for five years beginning on the date on which the transaction is completed. All other records will be kept for five years beginning on the date on which the business relationship ends.



Records will be kept in computerized or electronic form.



Company will ensure that all documents, data or information held in evidence of customer identity are kept up to date.

Copies of any SAR, together with any supporting documentation filed will be maintained for 5 years from the date of tiling the SAR.

All records will be handled in confidence, stored securely, and will be capable of being retrieved without undue delay.





## INTERNAL SUSPICION REPORTING

It is the policy of this company that MLCO shall remain alert for the possibility of money laundering, and shall report any and every suspicion for which he believes there are reasonable grounds, following the company's procedure.

### CONTROLS AND PROCEDURES

- MLCO must be alert for the possibility that the company's services could be used for money laundering purposes, or that in the course of his work company could become aware of criminal or terrorist property
- alertness to the possibility of money laundering must be combined with an appropriate knowledge of clients' normal arrangements so that MLCO becomes aware of abnormal factors which may represent possible causes of suspicion
- MLCO becoming aware of a possible suspicion will gather relevant information that is routinely available to them and decide whether there are reasonable grounds to suspect money laundering. Any additional CDD information acquired, in particular any explanations for unusual instructions or transactions, should be recorded on the client file in the routine manner, but no mention of suspected money laundering is to be recorded in any client file
- requirement to gather relevant information does not extend to undertaking research or investigation, beyond using information sources readily available within the company. Clients may be asked for relevant information, but only in the context of routine client contact relevant to the business in hand
- if after gathering and considering routinely available information, MLCO is entirely satisfied that reasonable grounds for suspicion are not present, no further action should be taken
- internal suspicion report does not breach client confidentiality, and no member of staff shall fail to make an internal report on those grounds
- if a suspicion report results from a matter raised by a member of support staff, the responsible solicitor must advise them in writing that a report has been submitted by reference to the matter discussed on the given date, without including the name of the person(s) suspected. This confirms to the member of staff who raised the matter that their legal obligation to report has been fulfilled
- If MLCO is aware of a suspicion of money laundering shall not discuss it with any outside party
- no copies or records of money laundering suspicion reports are to be made, except by the MLCO who will keep such records secure, and separate from the company's client files and other repositories of information

The following lists are not exhaustive but set out some of the main indications that a transaction is suspicious:

- new clients and 'one-off' transactions
- checking identity is proving difficult
- client is reluctant to provide details of their identity
- client will not disclose the source of funds
- explanation for the business and/or the amounts involved are not credible
- series of transactions are structured just below the regulatory threshold for due diligence identity checks
- client has made an unusual request for collection or delivery
- transactions having no apparent purpose or which make no obvious financial sense, or which seem to involve unnecessary complexity
- unnecessary routing of funds through third-parties

Regular and established clients:

- transaction is different from the normal business of the client
- size or frequency of the transaction is not consistent with the normal activities of the client
- pattern of transactions has changed since the business relationship was established
- money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the client's usual foreign business dealings
- sudden increases in the frequency/value of transactions of a particular client without reasonable explanation

Examples where client identification issues have potential to indicate suspicious activity:

- client refuses or appears reluctant to provide information requested
- there appears to be inconsistencies in the information provided by the client
- client's area of residence is inconsistent with other profile details such as employment
- address appears vague or unusual
- supporting documentation does not add validity to the other information provided by the client
- client is in a hurry to rush his activity through, with promises to provide the information later

Examples of activities that might suggest to staff that there could be potential terrorist activity:

- client is unable to satisfactorily explain the source of income or capital
- frequent address changes
- media reports on suspected or arrested terrorists

A Suspicious Activity Report (SAR) will be made to the NCA as soon as the knowledge or suspicion that criminal proceeds exist arises. The MLCO will be responsible for deciding whether or not the suspicion of illegal activity is great enough to justify the submission of a SAR.

## FORMAL DISCLOSURES TO THE AUTHORITIES

### POLICY

It is the policy of this company that the MLCO shall receive and evaluate internal suspicion reports, and decide whether a formal disclosure is to be made to the authorities. If so deciding, the MLCO will make the formal disclosure on behalf of the company, using the appropriate mechanism.

### CONTROLS AND PROCEDURES

- On receipt of a money laundering suspicion report from a member of staff, the MLCO shall acknowledge its receipt in writing, referring to the report by its date and unique file number. This confirms to the member of staff that their legal obligation to report has been fulfilled
- MLCO shall open and maintain a log of the progress of the report. This log shall be held securely and shall not form part of the client file
- following receipt of a report, the MLCO shall gather all relevant information held within the company, and make all appropriate enquiries of members of staff anywhere in the company, in order properly to evaluate the report. The MLCO shall then decide whether they personally believe there are reasonable grounds for suspicion, and make a decision on the company's obligation to make a formal disclosure to the authorities
- all members of staff, anywhere in the company, shall respond in full to all enquiries made by the MLCO for the purposes of evaluating a suspicion report. Information provided to the MLCO in response to such enquiries does not breach client confidentiality/professional privilege, and no member of staff shall withhold information on those grounds
- if deciding that a formal disclosure to the authorities is required, the MLCO shall make such disclosure by the appropriate means
- MLCO shall document in the report log the reasons for deciding to make or not to make a formal disclosure
- MLCO shall where appropriately inform the originator of the internal report whether or not a formal disclosure has been made
- MLCO shall inform all those, and only those, members of staff who need to be aware of the suspicion in order to protect them and the company from possible money laundering offences in connection with any related business
- following a formal disclosure, the MLCO shall take such actions as required by the authorities in connection with the disclosure

## STOPPING/CONTINUING WORK FOLLOWING A SUSPICION REPORT

### POLICY

It is the policy of this company that from the moment a suspicion of money laundering arises, no further work will be carried out on the matter that gave rise to the suspicion. Neither commercial considerations nor the difficulty in responding to the client's enquiries on the matter shall be permitted to take precedence over the company's legal obligations in this regard. In such circumstances the MLCO shall act with all possible speed to enable work to continue, or if appropriate to withdraw from the client relationship, and assist staff in any communications with the client affected.

### CONTROLS AND PROCEDURES

- as soon as a member of staff forms or becomes aware of a suspicion of money laundering, no further work is to be done on the matter giving rise to suspicion
- if there is any likelihood of the client becoming aware that work has stopped, for example because an anticipated transaction has not gone through, the member of staff concerned must contact the MLCO for instructions on how to handle the matter with the client
- on receipt of a suspicion report, the MLCO shall:
  - instruct the originator of the report and any other staff involved to cease work on the matter giving rise to suspicion
  - decide in the shortest possible time whether all work for the client concerned should be stopped, or whether other work that is not the cause of suspicion may continue, and advise relevant staff accordingly
  - assist all affected staff in handling the matter with the client so that no tipping off offence is committed
- when work for a client has been stopped, the MLCO shall carry out the evaluation of the suspicion report as quickly as possible to decide whether a disclosure must be made to the authorities
- if the MLCO decides that there are not reasonable grounds to suspect money laundering, he or she will give consent for work to continue on his or her own authority
- if the MLCO decides that a disclosure must be made, he or she will request consent to continue from NCA as quickly as possible
- if consent is refused by NCA, or delayed by an extension of the moratorium period, the MLCO will take advice from NCA and consult with the responsible solicitor on the company's continuation of or withdrawal from the client relationship

## AML TRAINING

The training of staff is not applicable at the moment as the business has only one employee involved in AML compliance who is also the MLCO and company owner. Company still has pre-set of basic policy to follow if employment will take place; until that all points are applicable as MLCO self-training. All affected employees are trained on their responsibilities in relation to money laundering legislation, and are aware of how to identify and deal with transactions that may involve money laundering - <https://www.politsei.ee/et/juhendid>

It is the policy of this company that all staff who have client contact, or access to information about clients' affairs, shall receive anti-money laundering training to ensure that their knowledge and understanding is at an appropriate level, and ongoing training at least annually to maintain awareness and ensure that the company's legal obligations are met.

## CONTROLS AND PROCEDURES

- All relevant staff will receive regular anti-money laundering training and/or e-learning and should ensure they are familiar with this policy. New joiners in roles that fall within this policy must complete training as part of the induction process and an e-learning module will be made available to this end
- MLCO will, in cooperation with the company's training officer, evaluate alternative AML training methods, products and services in order to make suitable training activities available to all members of staff who have client contact, or access to information about clients' affairs
- suitable training will take into account:
  - need to achieve a level of knowledge and understanding appropriate to the individual's role in the company
  - need to maintain that level through ongoing refresher training
  - practicality of assigning different program to staff with different roles on a risk sensitive basis
  - cost and time-effectiveness of the alternative methods and media available
- training program will include means of confirming that each individual has achieved an appropriate level of knowledge and understanding, whether through formal testing, assessment via informal discussion, or other means
- special consideration will be given to the training needs of senior management, and of the compliance team

- MLCO will:
  - inform every member of staff of the training program that they are required to undertake, and the timetable for completion
  - check that every member of staff has completed the training program assigned to them, issuing reminders to any who have not completed to timetable
  - refer to the business owner any cases where members of staff fail to respond to reminders and have not completed their assigned training
  - keep records of training completed, including the results of tests or other evaluations demonstrating that each individual has achieved an appropriate level of competence
- on completion of a training cycle, the MLCO will ensure the continuity of ongoing training while giving consideration to:
  - effectiveness of the program completed
  - need to keep training information up to date with changes in laws, regulations, guidance and practice
- MLCO will determine the training needs of his or her own role, and ensure that he or she obtains appropriate knowledge and understanding as required to fulfil the obligations of the appointment

## MONITORING AND MANAGEMENT OF COMPLIANCE

### POLICY

It is the policy of this company to monitor compliance with legal and regulatory AML requirements and conduct an annual independent AML compliance audit, the findings of which are to be considered and appropriate recommendations for action set out. The company's owner shall provide the necessary authority and resources for the ongoing implementation of a compliant AML regime.

### CONTROLS AND PROCEDURES

- MLCO will monitor continuously all aspects of the company's AML policies and procedures, together with changes and developments in the legal and regulatory environment which might impact the company's business-wide risk assessment
- any deficiencies in AML compliance requiring urgent rectification will be dealt with immediately by the MLCO, who will report such incidents to the company's owner when appropriate and request any support that may be required
- MLCO will facilitate and assist the independent auditor in conducting an annual audit of the company's AML compliance. This report might include:
  - summary of the company's money laundering risk profile and vulnerabilities, together with information on ways in which these are changing and evolving
  - summary of any changes in the regulatory environment(s) in which the company operates and the ways in which the company is affected
  - summary of AML activities within the company, including the number of internal suspicion reports received by the MLCO and the number of disclosures made to the authorities
  - details of any compliance deficiencies on which action has already been taken, together with reports of the outcomes
  - details of any compliance deficiencies on which action needs to be taken, together with recommended actions and management support required
  - outline of plans for the continuous development of the AML regime, including ongoing training and awareness raising activities for all relevant staff
- where management action is indicated, the company's owner will decide the appropriate action to be taken

## QUALITY CONTROL

Company must test the effectiveness of the checks they make and also the areas and indicators of risk that they have identified.

A review should include consideration of the following areas:

- are there any areas of weakness in the business where appropriate risk-sensitive checks are not being carried out in accordance with the MLR requirements and the business's policies and procedures?
- are correct records kept in respect of evidence of ID taken and other customer due diligence checks?
- are there any new products, services or procedures that require risk assessment, appropriate due diligence checks and internal controls putting in place?