CIDRUS SP. Z.O.O.

AML/CFT POLICY

1. INTRODUCTION

PURPOSE

This document sets out the principles and standards for compliance and management of risks associated with financial crime in Cidrus Sp z.o.o., incorporated in the Poland, Reg.No.0000969104.

The purpose of this document is to prevent the Cidrus Sp z.o.o. from being used for financial crime to comply with all applicable legal requirements and to ensure that the most appropriate action is taken by Cidrus Sp z.o.o. to mitigate the risks associated with financial crime.

This document outlines the applicable legal requirements related to financial crime to which the Cidrus Sp z.o.o. must adhere, as well as internal measures which are established by the Cidrus Sp z.o.o. to ensure it complies with these legal requirements. This document is referred to as the Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), Counter-Proliferation Financing (CPF) and Sanctions Policy (the Policy) and sets the parameters for the Cidrus Sp z.o.o. in relation to the AML, CTF, CPF and sanctions framework.

Scope and application

The Policy applies to all Cidrus Sp z.o.o. employees, all units in the Cidrus Sp z.o.o., senior management, foreign correspondents, contractors and third parties with whom Cidrus Sp z.o.o. may contract with. The aim of the Cidrus Sp z.o.o. is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to the Cidrus Sp z.o.o. of our customers using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or conduct prohibited financial sanctions activity.

The Policy is updated at least once a year, or more frequently based on international requirements and legislative changes.

Definitions

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

- Placement: Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.
- Layering: Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
- Integration: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

It also covers money, however acquired, which is used to fund terrorism. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Terrorist financing relates to the raising or holding of funds (directly or indirectly) with the intention that those funds should be used to carry out activities defined as acts of terrorism or with the intention to dispose those funds to a terrorist group or a separate terrorist.

Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Criminal property is the proceeds of criminal conduct. This includes any type of conduct, wherever it takes place, which would constitute a criminal offence if committed in Cidrus Sp z.o.o. It includes drug trafficking, terrorist activity, tax evasion, corruption, fraud, forgery, theft, counterfeiting, black mail and extortion. It also includes any other offence that is committed for profit.

Sanctions are political and economic decisions that are part of diplomatic efforts by countries, multilateral or regional organizations against states or organizations either to protect national security interests, or to protect international law, and defend against threats to international peace and security. Sanctions can be:

- Specific, i.e. relate to specific lists of named individuals, legal entities, organizations, vessels etc. (for example the US Department of Treasury refers to some of these entities as Specially Designated Nationals),
- General, i.e. cover all transactions with certain countries or jurisdictions; certain transactions with countries or jurisdictions such as exports, imports or new investment, or all transactions within a certain area of activity/products (for example arms sales to a particular country).
- Sectoral, i.e. cover certain parties in specific sectors (for example OFAC designates parties on a Sectoral Sanctions Identification List or "SSI List") but only restrict certain transactions of these designated parties.

These are terms you should be familiar with:

Terms / Acronyms	Definition
Nominated Officer	A Nominated Officer (also known as the MLR officer or AML Compliance Officer) is the focal point within the company for the oversight of all activity related to anti-financial crime issues.
Supporting Officer	A person or persons nominated to act on behalf of the Nominated Officer.
AML	Anti-Money Laundering
KYB	Know Your Business
KYC	Know Your Customer
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
PFIU	Polish Financial Intelligence Unit
Polish AML Act	Act on Counteracting Money Laundering and Terrorist Financing
PEP	Politically Exposed Persons
STR	Suspicious Transaction Report
Swift	Society for Worldwide Interbank Financial Telecommunications
OFAC	Office of Foreign Assets Control

Terms / Acronyms	Definition
FATF	Financial Action Task Force
UBO	Ultimate Beneficial Owner
EU	The European Union
UN	The United Nations
RBA	Risk Based Approach
CTF	Counter-Terrorism Financing
CPF	Counter-Proliferation Financing

2. AML PRINCIPLES

The purpose of the AML/CFT policy of Cidrus Sp z.o.o. is to establish the framework of the rules and procedures to be followed by Cidrus Sp z.o.o. to ensure that Cidrus Sp z.o.o., its resources, its business, its services and/or its employees are not directly or indirectly used or involved in moneylaundering or the funding of terrorism and that Cidrus Sp z.o.o. complies with all its legal obligations relating to the prevention of money laundering and funding of terrorism at all times.

This policy applies to all business activities of Cidrus Sp z.o.o. within the scope of its relevant financial business. This policy and its procedures are to be followed by all employees of Cidrus Sp z.o.o., who will be required to confirm that they have understood and will comply with their obligations under the AML/CFT procedures.

Cidrus Sp z.o.o. AML/CFT policy is set up to effectively implement, monitor, maintain and where necessary amend adequate procedures for the attainment of the AML policy's objectives. The AML policy shall be implemented on the basis of a risk-based approach. In this respect, Cidrus Sp z.o.o. shall conduct a risk assessment of its business, which shall be regularly reviewed, on the outcome of which Cidrus Sp z.o.o. AML/CFT procedures shall be based and, where necessary, adjusted.

Counteracting Money Laundering and Terrorist Financing (the "Polish AML Act") requires businesses to have appropriate systems of internal control and communication in order to prevent activities related to money laundering and terrorist financing. In simple terms this

means that businesses must ensure that management controls are put in place that will alert the relevant people in the business to the possibility that criminals may be attempting to use the business to launder money or fund terrorism or fund proliferation or violate sanctions, so as to enable them to take appropriate action to prevent or report it.

Systems of internal control and communication must be capable of identifying unusual or suspicious transactions or customer activity, of identifying transactions and business relationships. Cidrus Sp z.o.o. must report suspicious transactions under the Polish AML Act and associated Regulations.

The nature and extent of systems and controls that the business needs to put in place will depend on a variety of factors, including the:

- Degree of risk associated with each area of its operation
- Nature, scale and complexity of the business
- Type of products, customers, and activities involved
- Diversity of operations, including geographical diversity
- Volume and size of transactions
- Distribution channels.

Therefore, the Cidrus Sp z.o.o. has established internal controls procedure. The basis of the internal control process is well-defined authorizations, a segregation of duties, identification of clients, on-going due diligence, reporting suspicions, etc. The Cidrus Sp z.o.o. doesn't have an internal audit unit, however Cidrus Sp z.o.o. plans to carry out an auditing not less than once in two years, forming a group of three employees which are working in unrelated departments, unless it is assessed by the Cidrus Sp z.o.o. that a longer rotation cycle is appropriate. The decision of the participants of the formed group and the audit is made by the board of the company.

The Cidrus Sp z.o.o. regularly monitors changes in and compliance with relevant legislation and other legal requirements in order to mitigate money laundering and terrorism financing and proliferation financing and sanctions violation risks, as well as to make internal control procedures more efficient.

2.1. AML Program

Cidrus Sp z.o.o. has put into place the following components for an effective AML/CFT program:

- have an adequate management structure to supervise Cidrus Sp z.o.o. operations;
- designation of an MLRO and specification of his/her functions;
- cooperate with the competent authorities as may be necessary;
- monitor the financial transactions of its customers and detect and report any suspicious transactions;
- preserve all relevant information in its possession that may be required by the relevant authorities investigating a suspicious activity;

- implementation of necessary KYC/CDD procedures as required;
- Implementation of risk management procedures;
- Implementation of assessment and monitoring procedures of customer risk and payment risk indicators;
- Implementation of employees' AML training to ensure their awareness of the ML/FT risks, internal procedures as well as employee's obligations with respect of AML reporting;
- Implementing procedures for periodic re-assessment of Cidrus Sp z.o.o. activities and adjustment of policies and procedures as may be required to ensure that they are adequate at all times; and
- Record keeping of audit controls and decision making.

2.2. Policy Approvals, Revisions & Compliance Assurance

This policy and AML procedure and compliance thereto shall become applicable upon their approval by the Board of Directors. The re-assessment of the AML-related business risks, AML Policy and Procedures shall be carried out at least on annual basis or where otherwise required by a change in applicable legislation or a change in Cidrus Sp z.o.o. business. The review shall be driven by MLRO and presented to the Board of Directors on an annual basis. The AML Policy and Procedures shall be subject to planned and/or ad hoc audits carried out by the Internal Auditor of Cidrus Sp z.o.o. or by any other suitably qualified external entity as may be requested by the Board of Directors from time to time. Such audits shall test Cidrus Sp z.o.o. for compliance against the requirements of the Act, the AML Regulations and other applicable laws. Should an audit identify a compliance breach and/or any irregularity, these shall be formally reported to the Board of Directors for further investigation and timely rectification of identified non-conformances.

2.3. Risk Based Approach

Cidrus Sp z.o.o. shall adopt a risk-based approach ("RBA") in determining whether to accept or reject customers, and to assess the risks of its business, its customers and transactions as the basis for developing adequate measures and rules to prevent money laundering and funding of terrorism. A Risk-Based assessment enables a more targeted and focused approach to identifying and assessing risks that Cidrus Sp z.o.o. is or may be exposed to by applying resources to where they are most needed. The type of information required must therefore reflect the inherent level of ML/FT risk that each merchant represents. A robust RBA will therefore reduce the costs incurred as regards to on-going monitoring of client transactions and the procurement of paraphernal KYC documentation

2.4. Money Laundering Reporting Officer

A Nominated Officer is the person within an organization who is responsible for overseeing all activity related to anti-money laundering matters. In the absence of the Nominated Officer, Supporting Nominated Officers will take his/her place.

Cidrus Sp z.o.o. shall appoint and maintain an officer of Cidrus Sp z.o.o. to act as Cidrus Sp z.o.o. Money Laundering Reporting Officer (MLRO). The MLRO shall be an officer of

Cidrus Sp z.o.o. with sufficient seniority, education, reputable background, experience and command. Cidrus Sp z.o.o. Nominated Officers should remain up to date with AML/ATF rules and risks. The MLRO's responsibilities include:

- Receiving disclosures from employees (also known as Suspicious Transaction Report - STR);
- Reviewing all new laws and deciding how they impact on the operational process of the company;
- Preparing a written procedures manual and making it available to all staff and other stakeholders;
- Making sure appropriate due diligence is carried out on customers and business partners;
- Maintaining controls and procedures aimed at deterring criminal elements from using Cidrus Sp z.o.o. resources;
- Setting up, monitoring, updating AML/CFT procedures, including KYC, record keeping, risk assessment, STR escalation protocols;
- Receiving internal Suspicious Transaction Report (STR) from staff;
- Recording all decisions relating to STRs appropriately;
- Ensuring staff receive anti-financial crime training when they join and that they receive regular refresher training;
- Making decisions about continuing or terminating trading activity with particular customers
- Making sure that all business records are kept for at least five years from the date of the last customer transaction;

Cidrus Sp z.o.o. shall appoint a Supporting Nominated Officer to assist the MLRO in the fulfilment of his AML/CFT duties. The appointment of the designated employee shall in all cases receive the approval of the MLRO and shall work under his/her direction. All Employee shall immediately notify the MLRO if he/she suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur if a transaction is completed. Employees are encouraged to seek the assistance of the MLRO with any questions or concerns they may have with respect to the AML/CFT Policy & Procedures.

3. CUSTOMER DUE DILIGENCE

3.1. Identification and Verification

KYC means obtaining information about a customer over and above the required ID.

The Cidrus Sp z.o.o. has implemented a KYC program to ensure all kinds of customers (natural or legal persons or legal structures) are subject to adequate identification, risk rating and monitoring measures. This program has been implemented throughout all Cidrus Sp z.o.o. divisions. The purpose of this is to reduce the risk of the Cidrus Sp z.o.o. being used for money laundering and financing of terrorism.

Multiple online directories of individual and business information are used to check all customer/client ID details before a full Individual or Business e-account is activated.

For Business clients we also check their details against the public business registers (for example, Business Registers of the provinces and territories).

The following "Know Your Customer" procedures will be helpful in identifying prospective face-to-face or non-face-to-face customers who may present money-laundering and financing of terrorism and financing of proliferation risks. The Cidrus Sp z.o.o. applies a risk-based approach towards "know your customer" with reference to a customer's geographic ties, chosen products and / or services. A risk-based approach is applied as low, medium or high. This risk-based approach indicates the risk of whether the given customer may use or will use the Cidrus Sp z.o.o. services and/or products for financial crime.

In all cases, prior to taking on a new customer or engaging in a transaction with a customer with whom we do not have well-established relationship, the Cidrus Sp z.o.o. completes sufficient due diligence to have confidence in the integrity of the customers and the lawfulness of the proposed transaction by following actions:

1. Make reasonable efforts to determine the true identity of all customers and the legal and beneficial ownership of all accounts.
2. Determine the customer's citizenship, home and business addresses, occupation or type of business. Where appropriate, obtain supporting documentation.
3. Inquire whether the customer will have the sole interest in the account or whether there will be other persons who will have access to it. Verify the identity of all such persons and engage in any necessary due diligence regarding such other persons.
4. If the customer is not an individual;
   A. Determine the legal status (e.g., corporation, partnership or other form of entity).
   B. Determine whether the customer is regulated, either in the Poland or a foreign country.
   C. Determine all principal persons of the customer, such as officers and directors, or persons who have a substantial beneficial interest (i.e. own equal or more than 25% share in the company). As per the Polish AML Act Regulations, Cidrus Sp z.o.o. shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership. This includes details of beneficial interests held.
   D. Obtain copies of all relevant organizational documents.
5. Identify the source of the customer's funds.
6. Screen the customer for:
   A. Account holders from countries listed on the Financial Action Task Force ("FATF"), EU, UK, UN and other Sanctions lists;
   B. Persons with significant holding, that hold over 25% equity or more in a business are now subject to AML/CTF screening;
   C. Directors or people issued with Power of Attorney
   D. Sanctions match;
7. Where appropriate, obtain information regarding the frequency with which the customer expects to transfer funds to or from the account, i.e. monthly, quarterly, or the nature of any third-party payments to or from the account;

8. Where appropriate, obtain and contact reputable references, such as professionals and other members of the financial industry, banks, securities companies, etc.
9. Government Officials and Foreign Accounts.
Special procedures apply for accounts for the benefit of politically exposed persons (PEPs), including senior government and political figures, particularly from certain countries, and for accounts opened by or through foreign banks and for clients from countries or industries deemed high risk. The Cidrus Sp z.o.o. performs enhanced due diligence and on-going due diligence measures proportionate with the risk of the customer. High risk customers will therefore be subject to enhanced due diligence and on-going due diligence. On-going due diligence processes will be applied to all existing customers within a specific period that will be determined by whether they are defined as high, medium or low.

Each new business relationship must be reviewed according to the criteria as set forth under the law. This must be done before the establishment of the relationship or – where necessary for the continued normal conduct of business and provided that the AML/CFT risks are low and verification steps are completed as soon as reasonably practical – during the relationship being established.

In the event that, during an established relationship, doubts arise about the veracity or adequacy of previously obtained data, documents or information or changes have occurred, then the customer due diligence measures as described above are to be repeated.

3.2. Risk Qualifications

Cidrus Sp z.o.o. is at liberty to determine the extent of its customer due diligence measures on a risk sensitive basis, depending on the type of customer, business relationship, product or transaction. Certain types of businesses are more likely to be involved with money laundering and should be considered high risk. The AML Procedure and KYC/Onboarding Policy describes in detail which businesses are not accepted by Cidrus Sp z.o.o. (prohibited industries) and which are considered as high risk (restricted industries). The AML Procedure and KYC/Onboarding Policy provides a detailed description of matters relating to identifying and verifying a potential business relation with a merchant.

3.3. Enhanced Due Diligence

Apart from the business, there are circumstances where the risk of money laundering or terrorist financing is higher, such as (but not limited to):

- Country: Countries where merchant is located that are:
  - subject to sanctions, embargos or similar measures issued by the United Nations;
  - identified by FATF as non-cooperative;
  - identified by credible sources as:
    - not having adequate anti-money laundering/counter terrorist financing systems;
    - funding or supporting terrorist financing or that have designated terrorist organizations operating in that country;

    - having significant levels of corruption or other criminal activity;
    - having a non-transparent tax environment;
- The ownership structure appears unusual or excessively complex given the nature of the merchant's business;
- directors or ultimate beneficial owners identified as politically exposed persons; or
- transaction and merchant behavior (Is a risk posed by a merchant's behavior? What risk is posed by the products the merchant is using? To whom and where are the collected payments settled?).

In such cases extended customer due diligence measures have to be taken. Further reference is made to the KYC/Onboarding policy.

3.4. Simplified Due Diligence

On the other hand, there are also circumstances where the risk of money laundering or terrorist financing may be lower, such as (but not limited to):

- cases where the merchant is a financial institution subject to requirements to combat money laundering and terrorist financing (consistent with the FATF Recommendations) and are supervised;
- cases where the merchant is a public company listed on a stock exchange and subject to disclosure requirements to ensure beneficial ownership transparency;
- country: countries where merchant is located that are:
    - identified by credible sources as having effective anti-money laundering/counter terrorist financing systems;
    - identified by credible sources as having low level of corruption or other criminal activity.

In such cases, and provided there has been an adequate analysis of the risk, simplified customer due diligence measures may be taken. Note that a lower risk for identification and verification purposes does not automatically mean the same merchant is lower risk for all types of customer due diligence measures, for instance for ongoing monitoring.

4. MONITORING

Cidrus Sp z.o.o. is to conduct ongoing monitoring of its business relationships. Monitoring of customers shall be maintained on a risk-sensitive basis, and transactions shall be scrutinized to ascertain whether throughout the course of the relationship the transactions undertaken are consistent with Cidrus Sp z.o.o. knowledge of the customer's business and risk profile and the information provided to Cidrus Sp z.o.o. in the course of onboarding and carrying out KYC checks. Data and documents are to be kept updated, including identification documentation. Thus, the team shall monitor the transactions and upon discovery of a transaction of suspicious nature, an internal investigation shall be initiated. All Cidrus Sp z.o.o. customers are obliged to inform Cidrus Sp z.o.o. with regards to any changes within the corporate structure, directors, beneficial owners, registered address.

Besides above-mentioned, there is an ongoing due diligence implemented based on the client's risk level. It is carried out as following:

- Low risk clients: every two years;
- Medium risk clients: every year;
- High risk client: every six months.

4.1. Transaction Monitoring & Updating Files

Customer due diligence measures are to be applied by Cidrus Sp z.o.o. to existing customers on the basis of materiality and risk. Due diligence on existing relationships are to be conducted at appropriate times, taking into account any previous customer due diligence measures being undertaken and the adequacy of the information obtained then.

Cidrus Sp z.o.o. should have policies, controls and procedures in place that enables the effective management and mitigation of the risks that have been identified. Cidrus Sp z.o.o. should monitor the implementation of those controls and enhance them, if necessary. When assessing risks, Cidrus Sp z.o.o. should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied.

The risk assessment referred to above must also include the review and monitoring of the Money laundering and terrorist financing risks to the business. Cidrus Sp z.o.o. must conduct ongoing monitoring of their business relationships with their customers. Ongoing monitoring of business relationships means (i) transaction monitoring and (ii) up-to-date documents and information keeping.

Such review and monitoring, based upon a risk-based approach, will basically entail the monitoring of patterns for example a sudden increase in processing volumes, uncharacteristic transactions not in line with the known activities of merchants and strange peaks. The monitoring criteria, tools and measures are described in the AML procedure.

All personnel involved in monitoring for unusual or suspicious transactions or activities must be diligent in their monitoring activities. Sufficient tools are to be provided that should enable and facilitate monitoring to the fullest extent and that minimize any human failure as much as reasonably possible.

The systems of internal control and communication must be capable in meeting the requirements of identifying unusual or suspicious transactions or activities. Cidrus Sp z.o.o. must ensure that appropriate controls are put in place to lessen the risks as identified and prevent the business from being used for money laundering or terrorist financing. Managing and mitigating these risks must at least involve applying ongoing customer due diligence measures to verify the identity of the merchants and any ultimate beneficial owners:

- Obtaining additional information on high risk merchants;

- Conducting ongoing monitoring of transactions and activity of merchants;
- Having systems to identify and scrutinize unusual transactions and activity to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may take place.

Not only should ongoing monitoring reflect the monitoring of the merchant activities and transactions, but Cidrus Sp z.o.o. should furthermore implement means of assessing whether its risk mitigation procedures and controls are working effectively and where improvement is required. The relevant procedures need to be kept under regular review.

The reporting of unusual transactions/activity must comply with the Applicable Regulations and must be informed about all unusual transaction/activity.

5. POLITICALLY EXPOSED PERSONS

The definition of 'PEP' is set out below:

- Is or has, at any time in the preceding year, been entrusted with prominent public functions
- Is an immediate family member of such a person
- Is a known associate of such a person
- Is resident outside or within the
- Is or has, at any time in the preceding year, been entrusted with a prominent public function by:
  - Any state;
  - The European Community; or
  - An international body; or
  - Please note: An immediate family member or a known close associate of a person referred to in the paragraph immediately above does not necessarily qualify as a PEP without the appropriate risk assessment.

In cases where PEP is identified:

- Senior management approval should always be sought before establishing a business relationship with a PEP;
- The source of funds should be established.

The business relationship should be subject to enhanced and constant monitoring.

5.1.Establishing the source of funds

It is important that before a business relationship is entered into with a PEP their source of funds is stablished and Company is satisfied that there are no indications that funds that will be used for transactions to be carried out are derived from corruption (i.e. receipt of bribes), fraud or an attempt by the PEP to remove/hide assets from their home country.

The source of the PEP's funds may be established by asking the individual concerned a series of questions to determine from where they receive their money. These questions could include confirmation of the main source income (i.e. salary), any business interest or investments from which funds are/will be received.

5.2.Making a decision to transact with the PEP

Below are areas on which questions can be asked of the PEP to determine whether a business relationship should be established. Information from this can be presented to Senior Compliance Officer of Cidrus Sp z.o.o. them to make an informed decision:

- What is the position and the duties of the PEP- (please note that a less 'senior' PEP is less of a risk than heads of states, MP's, members of the Judiciary, Ambassadors)
- Are there any family members/close associates that are PEP's also?
- Identify the customer and the beneficial owner of the account.
- Know the customer's country of residence.
- Know the objective of opening the account and the volume and nature of the activity expected for the account.
- Obtain information on the occupation and the other income sources.
- Obtain information about the direct family members or associates who have the power to conduct transactions on the account.

6. IDENTIFICATION OF SUSPICIOUS ACTIVITY

Having identified a customer and conducted the necessary due diligence, we will be in a good position to spot anything unusual with the customers, their actions, inactions or transactions.

Look out for any suspicious actions or activity at every dealing stage with the customer. For example, this can be an unusual remittance abroad or a transaction amount that is not in normal line of activity.

The following list provides several types of behavior or activity that may be suspicious. The list is not exhaustive and not conclusive. Rather employees who have contact with customers, intermediaries or counterparties should use the list as a guide for inquiry and follow up:

- The customer wishes to engage in transactions that lack business sense or are inconsistent with the client's stated business/strategy.
- The customer exhibits unusual concern for secrecy, particularly with respect to his identity, type of business or dealings with companies.
- Upon request, the customer refuses to identify or fails to indicate a legitimate source for his funds.
- The customer exhibits an unusual lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to operate as an agent for an undisclosed principal but is reluctant to provide information regarding the principal.

- The customer has difficulty describing the nature of his business. The customer lacks general knowledge of his industry.
- For no apparent reason the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a haven for money laundering.
- The customer, or a person publicly or known to be associated with the customer, has a questionable background including prior criminal convictions.
- The customer account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.
- The customer account shows numerous currencies or cash transactions aggregating to significant sums. This is however not relevant as Cidrus Sp z.o.o. does not have any cash transactions.
- The customer account has a large number of wire transfers to unrelated third parties.
- The customer account has wire transfers to or from a bank-secrecy haven country or country identified as a money laundering risk.
- The customer account has unusual transactions or transactions that are disproportionate to the customer's known business.

Suspicious transactions with more specific ML/TF indicators related to MSB:

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Customer wants to pay transaction fees that exceed the posted fees.
- Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Customer enters into transactions with counter parties in locations that are unusual for the customer.
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.

Note: DO NOT raise any concerns with the customer or use words to suggest you are not happy with anything that may tip them off.

7. REPORTING PROCEDURE

Anti-money laundering processes require a team approach. Money laundering issues are complex. The Nominated Officer of Cidrus Sp z.o.o. should not attempt to shift through them alone and if the officer becomes aware of any suspicious circumstances, or have any questions, the officer should promptly consult with the Nominated Officer and Compliance Team of Cidrus Sp z.o.o.

Suspicious Transaction reports – internal company process. In the situation that an employee (for this purpose, collectively, staff members) has suspicions about a customer and/or transaction, he must ensure that the company Nominated Officer is notified about his suspicions as soon as possible.

The STR should contain as a minimum the following information:

- Details and identification data of all parties to the transaction
- The owner of the monies in question
- How the identity of the client was verified
- A full description of the transaction
- Reason for suspicion and supporting evidence
- Details of any assets which are subject to international sanctions

If in doubt, the staff member should call the Nominated Officer to discuss the reasons for their suspicion – however, they should be careful not to do this whilst the customer is standing in front of them or via any communication exchanged with the customer (they may 'tip off' the customer otherwise, see below).

The timing for submitting the internal STR is important. The law states that an individual working in the regulated sector should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

Where a staff member becomes aware that a customer wants to carry out a transaction which is suspicious and the timing for the transaction allows it, the staff member must ensure that 'consent' is given before processing the transaction. 'Consent' means that the company has sought and obtained approval from the regulator to process the transaction. Further information on 'seeking consent' is provided below.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company Nominated Officer. Once the Nominated Officer receives the internal STR from the staff member, the Nominated Officer has two options:

1. Report the STR on to PFIU (see procedure below);
2. File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to PFIU.

The Nominated Officer should complete the Nominated Officer STR Resolution form (see appendix for sample) in the event he decides not to make a report to PFIU.

7.1. Tipping Off

Any staff member needs to make a judgement as to whether any delay to the transaction ('consent request') would have the effect of 'tipping off' the customer. It is a criminal offence under section 333 of the Proceeds of Crime Act 2002, to do or say anything that might either 'tip off' another person that a disclosure has been made or in any way prejudice an investigation. This means that businesses must not tell a customer:

prejudice an investigation. This means that businesses must not tell a customer:

- that a transaction was/is being delayed because consent from PFIU has been requested;
- that details of their transactions or activities will be/have been reported to PFIU that they are being investigated by law enforcement.

In situations where delaying a transaction may inadvertently lead to 'tipping off', it will make sense to process the transaction and then ensure that a STR is submitted to the Nominated Officer as soon as possible after. The staff member will have the protection of the law as soon as a STR has been submitted to the Nominated Officer.

If in doubt about whether to proceed with a transaction, the staff member should immediately contact the Nominated Officer for advice.

Supporting documentation is a cornerstone of our anti-money laundering and counter terrorism financing procedures. Unrecorded steps are soon forgotten. Records assist in tracking relevant information and in demonstrating that the company/individual has conducted our business responsibly and with integrity.

All interviews, searches and activities undertaken to verify integrity of transactions and persons must be documented and stored for reference by Cidrus Sp z.o.o., PFIU if and when required. All records must be kept for a minimum of five years after the business relationship with the customer ends.

Cidrus Sp z.o.o. must be able to demonstrate its compliance with the Applicable Regulations, by means of keeping evidence and records of due diligence checks made and information held on merchants and transactions. The following records are to be kept:

- All documents obtained for the purpose of identifying the merchant and the ultimate beneficial owners;
- Verification evidence on the identification documents obtained and the resolution of any discrepancy in the identifying information;
- Supporting records in respect of the business relationships;
- Results of credit analysis or any other analysis undertaken;
- Transaction data must be maintained in a form that can easily be compiled for an audit trail and which establishes the right transaction profile of the merchant;
- All other information related to money laundering matters.

Records are to be kept for at least five years, beginning either on the date on which (i) the business relationship ends for all customer identification/due diligence records and (ii) the transaction is completed for all transaction records.

8.1. Record Sharing

Cidrus Sp z.o.o. will share AML information (customer identification, due diligence and transaction records and other relevant information) with the FIU, law enforcement authorities and other financial institutions, if it is requested to do so. Cidrus Sp z.o.o. will

maintain procedures to protect on one hand the security of requests from such authorities, but on the other hand not unnecessarily jeopardize the confidentiality rights of the merchants.

Cidrus Sp z.o.o. will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain a business relationship or engage in a transaction. Furthermore, upon request, Cidrus Sp z.o.o. may be required to submit periodical reports on its policies, procedures and other information, in a format as required by the FIU.

9. STAFF AWARENESS AND TRAINING

The MLRO shall make sure that initial and on-going training is provided to employees, at least annually, to ensure that all relevant staff is aware of the regulatory obligations of Cidrus Sp z.o.o. under the Applicable Regulations, their personal responsibilities and how to recognize and handle suspicious transactions.

Compliance team including any other customer-facing and/or transaction- facing employees whose duties include the handling of relevant financial business or activity as defined under the Applicable Regulations shall receive more detailed training about Cidrus Sp z.o.o. AML procedures with respect to identifying clients, monitoring, record-keeping, remaining vigilant at all times, and reporting any unusual/suspicious transactions. Training logs will be maintained.

Cidrus Sp z.o.o. maintains an on-going employee training program so that the staff is adequately trained in KYC procedures and that the staff is aware of different possible patterns and techniques of money laundering which may occur in their everyday business. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers/Merchants. New staff is educated in the importance of KYC policies and the basic requirements at the Company. Training is given to all staff members upon commencement of taking on the position in the Cidrus Sp z.o.o. and on regular occasions afterwards (at least once a year).

Staff members who deal directly with the customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an on-going basis and to detect patterns of suspicious activity. Training also covers the general duties arising from applicable external (legal and regulatory), internal requirements and the resulting individual duties which must be adhered to in everyday business as well as typologies to recognize money laundering or financial crime activities or sanctions violation typologies.

Regular refresher training is provided to ensure that employees are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within services that promotes such understanding is the key to a successful implementation.

Training covers the following issues:

- The law relating to financial crime;
- Risks associated with the financial crime threat to the company (see, for example, www.egmontgroup.org);
- Identity and responsibilities of the Nominated Officer;
- Internal policies and procedures put in place;
- Customer Due Diligence/Enhanced due diligence monitoring measures;
- Suspicious activity – what to look out for;
- How to submit an internal Suspicious Transaction Report to the Nominated Officer;
- Record-keeping requirements;
- Possible sanctions violation – what to look out for.

The Nominated Officer will keep a log of all training which is provided to staff members. All staff will be required to sign the training log where required to confirm that they have received training. The Nominated Officer will circulate to all staff other material to heighten awareness of anti-financial crime issues. This must be placed on the company notice board which should be available in all company's locations.

The Nominated Officer shall be responsible to include information in respect of his/her education and training program(s) attended during the year in his/her Annual Report.

9.1.Role of the Employee

In the situation that an employee has suspicions about a customer and/or transaction, he must ensure that the company Nominated Officer is notified about his suspicions as soon as possible. Staff should use the internal 'Suspicious Transaction Report Form' (see appendix for example). The STR should contain as a minimum the following information:

- Date/time of transaction
- Amount
- Customer name/customer ID information (e.g. passport number, etc.)
- Transaction number
- Reason for suspicion of transaction

If in doubt, the staff member should call the Nominated Officer to discuss the reasons for their suspicion– however, they should be careful not to do this whilst the customer is standing in front of them (they may 'tip off' the customer otherwise, see below). The timing for submitting the internal STR is important. The law states that an individual working in the regulated sector (i.e. EMI or API) should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards. However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the

of the law, once a report of their suspicions has been made to the company Nominated Officer. Once the Nominated Officer receives the internal STR from the staff member, the Nominated Officer has two options:

- Report the STR on to PFIU
- File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to PFIU. The Nominated Officer should complete the Nominated Officer STR Resolution form in the event he decides not to make a report.

ANNEX 1 – Risk Appetite

1. Prohibited Businesses, Activities

The company has set itself the prohibition of the list of goods and services (industry):
1. Banknotes sales;
2. Drugs and the use of a drug or drug-like substance;
3. Arms and ammunition;
4. Jewelry, precious metals;
5. Reinsurance and insurance services;
6. Binary Options;
7. Multi-level marketing (MLM);
8. Antiques and art trade;
9. Pharmacies and pharmaceutical activity, pharmaceutical, proprietary medicinal products and pharmaceutical trade;
10. The sale of tobacco products;
11. Illegal / piracy audio or video recordings;
12. Infringing goods (counterfeit goods);
13. Sexual services, Adult;
14. Financial pyramid;
15. Debt collection services;
16. Accept assets that are known or suspected to be the proceeds of criminal activity;
17. Enter into/maintain business relationships with individuals or entities known or suspected to be a terrorist or a criminal organization or member of such or listed on sanction lists;
18. Maintain anonymous accounts, accounts for shell banks or pay-through accounts.

2. Prohibited Countries

In accordance with the international regulatory obligations, as well as its high-quality level standards, Cidrus Sp z.o.o. is not operating or have any kind of business relationships with persons, or process incoming/outgoing transactions related to Prohibited Countries. This list is fixed by Cidrus Sp z.o.o. and is subject to regular change.

Afghanistan	Barbados	Belarus	Botswana
Burkina Faso	Burma	Burundi	Cambodia
Cayman Islands	Central African Republic	Crimea	Democratic People's Republic of Korea (DPRK)

Afghanistan	Barbados	Belarus	Botswana
Burkina Faso	Burma	Burundi	Cambodia
Cayman Islands	Central African Republic	Crimea	Democratic People's Republic of Korea (DPRK)
Democratic Republic of the Congo	Ghana	Haiti	Iran
Iraq	Jamaica	Lebanon	Libya
Mali	Mauritius	Morocco	Myanmar
Nicaragua	Pakistan	Palestine	Panama
Philippines	Russia	Senegal	Somalia
South Sudan	Sudan	Syria	The Bahamas
Trinidad and Tobago	Uganda	Ukraine (Donetsk and Luhansk)	Venezuela
Yemen	Zimbabwe		

AANNEX 2 - Internal Suspicious Transaction Report Format

SAR No.:...../.....

Particulars	**Remarks**
Date:	
ID of the customer:	
Name/address of Customer:	
Telephone no of Customer:	
Nature of suspicious activity:	
Give full detail of suspicion: [Include detail of transactions and identity checks.]	
Attach any relevant documents: 1. Transaction receipts 2. Proof of ID and Address 3. Sanctions list checks	
Name of the Reporting Officer:	
Signature by Reporting Officer:	
Refer to PFIU: [To be completed by Nominated Officer]	
Do not refer to PFIU: Reason for decision: Details	
Signature by Nominated Officer:	
Date referred to Nominated Officer Decision:	