Policy 2023

Anti-Money Laundering and CTF (AML / CTF)

Table of Contents

1 OBJECTIVE AND SCOPE OF THE POLICY

The objective of this policy is to govern Six Seasons GmbH (hereinafter referred to as the "Company") measures to the application of legal and supervisory provisions to combat money laundering and terrorist financing and corresponding duties of care.
The Company carries out remittance money transfers as an agent using partner systems and receives commissions for these transactions as stipulated in the respective agency contracts. The Company is established and authorized under the laws of the Swiss Confederation and, therefore, falls within the definition of a financial intermediary within the scope of Article 2 paragraph 3 of the Anti-Money Laundering Act - AMLA of the Swiss Confederation.

Money laundering and terrorist financing have been identified as significant threats to the money remittance industry and the international financial services community. In line with many other countries, Switzerland has passed legislation designed to prevent money laundering and combat terrorism. This legislation, together with a variety of regulations, rules, and industry guidance, forms the cornerstone of AML/CTF obligations for Swiss firms and outlines the offenses and penalties for failing to comply. The requirements of Swiss legislation apply to Six Seasons GmbH and its partners. Six Seasons GmbH, at its sole discretion, may have established additional policies and procedures to comply with the Federal Anti-Money Laundering Act legislation, regulations, and any SRO PolyReg-approved guidance. Six Seasons GmbH is a registered Limited Liability Company in the Canton of Zürich and a member of SRO PolyReg.

This policy is focused on the key risks allocated to the Compliance Function as identified based on the key activities of the Company. This policy outlines the respective controls and further monitoring and reporting measures in order to mitigate risks resulting from potential money laundering and the financing of terrorism through the Company.

The Company is committed to complying with all applicable Swiss laws and regulations relating to AML/CFT and based on the PolyReg Reglament.

1.1 Applicability of this Policy

This internal policy applies to all activities of the Company. It forms part of the Company's governance framework and it applies to all employees, contractors, and volunteers in Switzerland and abroad ("Employees").

2 COMPLIANCE FUNCTION/CMPLIANCE UNIT

As an independent control function, the Compliance Unit monitors compliance risks and adherence to corresponding legal, regulatory and internal regulations. While complying with the legal procedures and implementing the AML measures, Employees, depending on their position and functions within the Company, must comply with the following procedures described in detail further in these Procedures:

- identification and verification of Clients and Beneficial Owners;
- ML and TF risk assessment and risk management;
- organization of ongoing monitoring;
- implementation of international financial sanctions and restrictive measures;
- submission of reports and information to the Money Laundering Reporting Office Switzerland (MROS) and PolyReg;
- management of Registers;
- safekeeping of the information;
- updating of the Client and the Beneficial Owner identification information;
- organizing trainings for Employees in order to properly acquaint them with the requirements for the prevention of AML;
- distribution of functions in the implementation of ML and TF prevention measures by the Company, as well as management and communication of information on compliance with the requirements.

3 PROCEDURES

3.1 KYC Procedures (Clients Due Diligence)

Client Due Diligence (“due diligence” or “CDD”) process must comply with procedures as detailed herein. These include the identification of the Client, ML and TF risk assessment, the assessment of the financial position of the Client, the validity of the identification, and the source of funds.

The following procedures, which constitute the ML and TF prevention measures, shall be carried out in order to perform customer due diligence procedures when performing Money Remittances or Money Exchange:

- the identification of persons, who apply to the Company as potential Clients;
- the identification and verification of the identity of the Beneficial Owner, if applicable;
- obtaining information on the purpose of the transaction and the intended nature of the relationship with the Company;

3.2 The identification of the clients

a) In compliance with the provisions of Chapter 2, section 1 of the Anti-Money Laundering Act (AMLA), the Company requires a good working knowledge of the Client's activities in order to provide an effective service, including evidence of their identity. The Company needs to identify the Clients and confirm that they are also the Beneficial Owners of the funds in the following circumstances:

- before establishing a Business Relationship
- when performing Cash Money Remittance, Online Money Remittance services, or Currency Exchange services for any amount;
- when there are doubts about the veracity or adequacy of previously obtained identification data of the Client and/or the Beneficial Owner the identification needs to be repeated;
- in any other case when there are suspicions that the act of ML or TF is, was or will be performed.

b) If in the course of undertaking a Monetary Operation or Transaction or Money Remittance or Money Exchange, the final amount of the Monetary Operation or Transaction or Money Remittance or Money Exchange is not known, the Company identifies the Client immediately after establishing that the amount of the Monetary Operations or Transaction or Money Remittances or Money Exchange is equal to or exceeds the amounts specified in Annex I.

c) In all cases when the identity of the Client and the Beneficial Owner is established, the Company obtains from the Client the information about the purpose and intended nature of the Client's intended transactions.

d) The Company in all cases conducts the ongoing monitoring of the Client's Business Relationship, including scrutiny of transactions undertaken throughout the course of that

relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Client, the business and risk profile, and the source of funds.

e) To ensure that the documents, data or information provided during the identification of the Client and the Beneficial Owner are appropriate and relevant, they are reviewed and updated by the Company on an ongoing basis.

f) The Company applies the Client and Beneficial Owner identification measures not only to new Clients but to the existing Clients as well, on a risk-sensitive basis, upon the occurrence of new circumstances or subject to new information related to the establishment of the risk level, identification-related information, their activities and other significant facts, and also in such cases when there is the obligation to submit information under Chapter 2, Sections 1 and 2 of the Swiss Anti-Money Laundering Act (AMLA) and PolyReg Reglamant.

g) The evidence of the identification must be obtained before the provision of any services to a prospective Client or an established Client – if sufficient evidence cannot be obtained the Company must not proceed with the business.

3.3 Client Manager function (front)

Client facing Employees i.e. Client Managers ("CM") and all other Employees with access to client or transaction data, are responsible in the first instance for complying with the obligations to exercise due diligence in line with this Policy.

The CM's are responsible for the following:

- obtaining all necessary documents for High-Risk Clients and preparation of the necessary background reports;
- conducting regular reviews of Clients in a frequency commensurate with the risks and reporting any significant changes to Compliance;
- Organize clients KYC documentation and keep it in order
- Timely informing Compliance Function in the event of suspicion of a qualified tax offence and preparation of a corresponding background report.

3.4 Identification methods

a) Clients may be identified by means of face-to-face contact or using non-face-to-face identification methods. This also applies to the cases where the Client, either natural or legal person, is represented by another person.

b) In case of Cash Remittances or Currency Exchange, the Company identifies its Clients through face-to-face contact. For Cash Remittance or Currency Exchange services the Company serves only natural persons. The Company requests original identification documents or authenticated copies thereof. The Company shall place the authenticated copies in his files or creates a copy of the original document presented. The Company must confirm with signature and date on the photocopy that the document originally inspected was the original or an authenticated copy. In case of Online Remittances, the Company identifies its Clients using non-face-to- face identification methods in accordance with the FINMA Circular 2016/7 on Video and online identification. For Online Remittance services the Company serves only natural persons.

c) In the case of the Business Relationships, the Company identifies its Clients using non-face-to-face identification methods.

3.5 Employees

All Employees must:

- acknowledge that failure to comply with this policy can result in regulatory or legal measures against the Company and its Employees and that, in addition, internal sanctions may be imposed;
- acknowledge that maintaining relationships with clients that violate applicable laws and regulations, or Employees deliberately concealing known or suspected violations of these laws and regulations, could hazard the Company's reputation and its ability to continue as a going concern and are therefore to be classified more critical than a potential loss of a business relationship.
- not accept, either intentionally or through negligence, funds which are the proceeds of crime, corruption, misuse of public assets, abuse of authority or abuse of office or qualified tax offence;
- not maintain business relationships with persons or companies where the Company knows or must assume that the company or person in question finances terrorism or is a criminal organization, or is a part of or supports such an organization;

4 DEFINITIONS OF BUSINESS RELATIONSHIPS AND RISK FACTORS

Based on Article 13 AMLO-FINMA, and PolyReg regulations, the Company is required to develop criteria for the identification of high-risk relationships. The Company has specified risk criteria using a risk-oriented approach, which divide all business relationships into three risk categories: Low-, Medium- and High-Risk Clients. The classification is based on systematic risk scoring within by manual adjustment of the proposed risk category.

For each new business relationship to be established or as part of the periodic reassessment process, clients are assessed in terms of their risk profile using risk scoring principles according to the nature:

a) client risk;

b) countries and geographical areas risk;

c) products and services risk;

d) delivery channel risk.

The general assessment of all risks shall be based on risk factors that are common to the whole base of the Company’s Clients, countries and geographical areas, products, services and Monetary Operations or Transactions or Money Remittances or Money Exchange, delivery channels.

The following processes and procedures, applicable to the Company's risks in general, will be used for ML and TF risk mitigation purposes:

- conducting a formalized risk assessment with respect to the Company's ML and TF risks at least annually. This assessment will include the identification, prioritization, measurement and categorization of ML and TF risks;
- the Company's Employees will be trained to acknowledge ML and TF risks related to their work, to detect them and to report thereon to the Compliance Unit;
- continuous monitoring of ML and TF risks and controls and implementation of the appropriate risk mitigation mechanisms where necessary;
- formalizing responsibilities of the key Employees for managing ML and TF risks;

4.1 Prohibited relations.

The Company considers the following Clients as prohibited clients in case of Cash Remittances or Currency Exchange and does not provide services to them:

a) Clients who are PEPs, or Close Associates or Close Family Members of a PEP;
b) Clients who are natural persons residing in the high-risk third countries entered on the lists of states published by the FATF that have serious deficiencies in the field of prevention of ML and/or TF and combating these crimes;
c) Clients who are subjects to international financial sanctions;
d) Clients who have been reported to the MROS by the Officer at least once due to the suspicious activity;
e) Clients who are residents in heavily sanctioned jurisdictions from the FATF Blacklist at the time the Cash Remittances are performed;
f) Clients who are under 18 years old;
g) Clients who have no legal ground to reside in Switzerland and or to travel here (without visas);
h) Clients acting through the representative and/or Clients who are not final Beneficial Owners itself;
i) Clients who are linked with any jurisdiction that is a high-risk country according to FATF, Switzerland or EU Commission;
j) Clients who are in the list of not the Special Interest Persons (SIP): natural persons who are reported in publicly available sources as being accused of or convicted of serious crimes, including financial crime, organized crime, terrorism, narcotics crime, and other crimes.
k) if checks in the additional sources reveal that the data of the Client conform to the data of the persons associated with the ML/TF as specified in the respective lists of the Swiss Confederation, EU, FATF or the United Nations;
l) Client who is non-compliant with these Procedures;
m) if the Company is unable to verify the identity of the Client in accordance with these Procedures;
n) Clients who fail to provide documents or information requested for identification purposes;
o) if doubts regarding the correctness or authenticity of the documents or information provided by a prospective Client arise;
p) Clients' activities or the origin of wealth and funds have harmed/are likely to harm the Company's reputation.

The Company will not carry out and will not allow illegal or unacceptable risk activities through the Company in the case of Business Relationships and considers the following Clients as prohibited clients and does not establish any commercial relationship services with them:

q) the Client is a shell bank or is owned by more than 25% of an entity identified as a shell bank;

r) the Client is engaged in the activity of arms, defense, military;

s) the Client is engaged in the activity of atomic power;

t) the Client is operating in extractive industries;

u) the Client is a regulated or unregulated charity;

v) the Client is a non-government organization or NPI;

w) the Client is engaged in the activity related to marijuana, cannabidiol products;

x) the Client is an embassy/consulate;

y) the Client is engaged in the activity of gambling;

z) the Client or his Beneficial Owner is subject to international financial sanctions (UN, EU Consolidated lists, OFAC);

aa) the Client is the natural person/legal entity residing/registered in or his Beneficial Owner is from high-risk third countries determined by the European Commission;

bb) the Client is the natural person/legal entity residing/registered in or his Beneficial Owner is from the high-risk third countries entered on the lists of states published by the FATF that have serious deficiencies in the field of prevention of ML and/or TF and combating these crimes;

cc) the Client is engaged in activity related to illegal goods and counterfeit goods;

dd) the Client has been reported to the MROS by the Officer at least once due to the suspicious activity;

ee) the Client is engaged in any other types of businesses that are involved in any form of criminal activity;

ff) the Client who residents in in heavily sanctioned jurisdictions from the FATF Blacklist;

gg) the Client who is non-compliant with these Procedures;

hh) if the Company is unable to verify the identity of the Client in accordance with these Procedures;

ii) Clients who fail to provide documents or information requested for the identification purposes;

jj) if the doubts regarding the correctness or authenticity of the documents or information provided by a prospective Client arise.

These lists of prohibited Clients are not exhaustive and can be amended or expanded depending on the results of the regular Company-wide risk assessment. Other Clients may be included in a case-by-case decision made by the Compliance Unit.

4.2 Implication of Due Diligence Standards

After the risk assessment is performed, the Client is assigned to one of these three categories according to its risk profile:

- **Low Risk Clients** – the standard due diligence and AML prevention measures may apply;
- **Medium Risk Clients** – the standard due diligence and AML prevention measures apply together with requests for additional information;
- **High Risk Clients** – the EDD and AML prevention measures apply;

The classification of the Clients in the risk assessment is not static, if information appearing during the due diligence indicates a higher risk than initially assessed, the level of due diligence must be corrected to the appropriate level. The detailed description of the individual risk assessment of the Client is provided in Annex I.

4.3 Enhanced Due diligence process

The Company applies enhanced due diligence procedures in the following cases:

- if a Client all time transacted amount accumulates to more than CHF 5'000 per year.
- if a Higher risk of ML and/or TF is established according to the risk assessment and management procedures set by the Company (High-Risk Clients);
- in the case of performance of transactions or Business Relationships with PEPs. But the Company not provide services to PEP in general.

High-Risk Clients are those Clients who are assigned to this category after the risk assessment or due to the results of the ongoing monitoring.

If the Client requires Enhanced Due Diligence ("EDD"), apart from normal due diligence procedures, the following additional measures must be taken:

- The EDD form will be filled out by clients;
- The EDD from will be assess by Relations Manager (front) and in case by case basis additional information might be requested from client.

The Compliance Unit together with Management have developed a special thresholds and KYC requirements
The Client identified as a High-Risk are subject to the Enhanced Due Diligence ("EDD"). The EDD is performed If for Low and Medium risk clients if Cash Remittance of one or several transactions, equivalent or exceed a sum of CHF 5,000 in one calendar year.

The EDD includes collection of filled out EDD form but not limited to the collection and documenting the origin of the funds. The Client may be asked to provide one of the following documents subject

to case by case check:

a) salary/pay slip;

b) job contract;

c) bank account statement at least for the last 4 months as a proof of salary or savings;

d) dividends certificate;

e) proof of the sale of movable property and real estate;

f) bank loan agreement;

g) other proof of the source of the funds, for example, tax return;

h) proof of the purpose of incoming Cash Remittance, for example, sale contract.

The Client is asked to send the additional documents e-mail or come to the Company's office to present it or give it to the Clients Manager or Employee of the Company to scan it.

5 RULES OF IDENTIFICATION OF PEP

1. At the beginning of a Business Relationship when registering the Client and before performing Money Remittances or Money Exchange, it is necessary to determine whether the Client should be included in the category of PEPs.
2. The Client together with all required information during the KYC procedure also provides the Company with Yes/No PEP declaration. When carrying out the Client verification, the Client is required to indicate if he/she is a PEP category.
3. When registering a new Client and before performing Money Remittance, the Company performs a check of the provided information, including the correctness of the information provided and PEP screening. The Client's data is automatically verified against an independent commercial PEP register and lists obtained from a reliable and independent source provided by the third parties. Checks are made through a secure web-based platform, which receives daily updates. It provides role-based access and workflow, single and batch scanning of person and

organization names, complex scanning and matching algorithms, comprehensive reporting and research material.

4. In case of doubt the Company requires a Self-declaration by the Client of their PEP status (i.e. by disclosing present or former employment or principal occupation clearly recognizable as a PEP).
5. If the Client is included in the PEP category (i.e., a natural person, is identified as a PEP or PEPs are identified in the management structure of a Client that is a legal entity) and in case of a proven PEP match (80% and more possibility of a match):
   5.1. in case of Money Remittances or Money Exchange, the Client will fall into the category of prohibited Clients and will not be served with Money Remittance services (these Clients are automatically rejected);
   5.2. in the case of Business Relationship, the Client will fall into the category of high-risk Clients and will be subject to enhanced due diligence. The Client's reputation will be checked, and consideration will be given to the need to obtain evidence of the Client's source of wealth and source of funds, as well as any other documents or information that may be required to evidence the legality of the Client's transactions and activities.
6. Establishing or continuing a Business Relationship with the Client that is included in the PEP category is only permitted upon obtaining written consent from the Officer. Enhanced monitoring will be applied to transactions and activity of the Client that are included in the PEP category.
7. Checking the Clients for PEP is also performed through ongoing monitoring and when the information about the Client is updating.

6 HIGH-RISK TRANSACTIONS

Based on article 14 AMLO-FINMA, the Company shall develop criteria to recognize high-risk transactions. Identified High-Risk Transactions must be adequately investigated and documented. Clients Manager and other Employees must investigate supposedly High-Risk Transactions. The primary responsibility for validating High-Risk Transactions is allocated with the Clients Manager.

6.1 Definition of High-Risk Transactions

The financial intermediary shall establish criteria for recognition of transactions with higher risk. Depending on the business activities of the financial intermediary, indications for higher risk are:

- the amount of the assets or the nature and volume of the transactions that appears unusual, considering the customer's profile or the circumstances; especially when there are indications of money laundering within the meaning of AMLO-FINMA, without a clear explanation;
- considerable deviations that are noted from the customary transaction nature, volumes and frequencies, considering the specific business relationship or in comparable business relationships;
- country of origin or destination of payments, particularly payments from or to a country considered as “high risk” or non-cooperative by the FATF.

The following are considered transactions with higher risks in any case:

- Transactions in which at the beginning of the business relationship assets in value of more than CHF 100’000 are physically paid in at once or gradually;
- Payments from or to a country considered as “high risk” or non-cooperative by the FATF and for which the FATF calls for increased diligence;
- In regards to money or asset transfers one or more transactions, which appear interlinked, amount to or exceed a sum of CHF 5'000.

7 DOCUMENTATION (“CLIENT FILE”)

The opening of a client or prospect must be documented and stored.

Identification Documents (copies):

a) Passport, identity card, Swiss driving license or some similar document with personal signature
b) Passport without signature require additional official document with signature
c) Proof of Address;
d) In case of Enhanced Due Diligence, the Client maybe asked to provide at least one of the documents listed below as a Proof of Address;
e) utility bill – not older than 3 months;
f) certificate of residence address;
g) bank statement – not older than 3 months;
h) lease agreement – not older than 12 months;
i) tax correspondence – not older than 12 months;
j) letter of employment – not older than 3 months;
k) a rental or mortgage contract or statement - not older than 12 months;
l) other proof of the residency.

7.1 Forms:

- **Form A:** Declaration of the Identity of the Beneficial Owner
- **Form K:** Establishing of the Controlling Person of operating legal entities and partnerships both not quoted on the stock exchange
- **Form R**: Declaration in connection with the opening of accounts held by lawyers and notaries or by a firm of lawyers or notaries licensed in Switzerland that are organized in the form of a company
- **Form S:** Foundations as well as similar constructs
- **Form T:** Declaration for trusts
- **Form I:** Information on life insurance policies with separately managed accounts/securities account (insurance wrappers)

The Company must demand a declaration using the correct Form published on PolyReg website in any case (i.e. independent from the type of client relationship).

The Relation Manager is responsible for creating and continuously updating the client File. The Relation Manager continuously supplements the client profile with essential information and changes that arise in the course of client relationship. Any changes in clients profile can only be made if all required documents and approvals are received.

7.2 Name Matching

The Relation Manager must insure that every business relationship prior to the establishment of the relationship by querying specialized databases and public sources (e.g. Google) in respect of negative news, sanctions or PEP status. The CM will check on the following persons:

- Account holders;
- Beneficial Owners;
- Directors (corporate accounts only).

Since the Company is working with Money Transferring Partners their systems can also be used to provide the screening results, thus such name matching process should be documented and available for the regulator at any time. Compliance Unit and Clients Manager must insure that each clients is scanned for sanctions and other statuses.
The Sanction Lists include as a minimum:

- The OFAC List;
- The SECO List;
- The consolidated EU Sanction Lists.

7.3 Identification of a legal person in case of the Business Partnership Relationships

The Company collaborates with existing licensed Money Transfer Operators (MTOs) located in Switzerland and abroad.
Business Relationships are identified in general through a non-face-to-face process. The identification can only be performed by authorized signatories or authorized representatives of the legal entity. After the Company identifies the Partner's authorized representative, the identification is performed in accordance with the requirements applicable to natural persons:

The Partner provides the following information in the KYC form:

- name of legal entity (including name in original language);
- legal form;
- registered and business address;
- registration number (if any);
- date of registration and extract from the register;
- e-mail, business telephone number, web address;
- business activity;
- information about the manager of the legal entity: forename, surname of the manager, personal number (if the customer is a foreign national – date of birth (if available – personal number or any other unique sequence of symbols intended for the identification

of a person)), nationality (if the person is stateless – the country which has issued the identification document);

The Partner uploads the following documents:

- <u>for Partners recorded in the Commercial Register:</u>
  - an extract from the Commercial Register issued by the Registrar; or
  - a written extract (procured by the Company) from a database managed by the registration authority; or
  - a written extract (procured by the Company) from a reliable, privately managed directory or database.
- <u>for Partner not recorded in the Commercial Register or an equivalent Register:</u>
  - the by-laws, founding acts or agreements, auditor's certification, official authorization to exercise the activity or equivalent documents; or
  - a written extract (procured by the Company) from a reliable, privately managed directory or database. Authorities must be identified by means of an appropriate by-law / resolution or other equivalent documents or sources. The extract from the Commercial Register, the certification by the auditor and the directory or database extract must be no more than one year old at the time of identification and must correspond to the current circumstances.

The Partner uploads identification documents of the Beneficial Owner – electronic copy of passport/ ID card. The company can choose to require the live video-streaming identification process for the Beneficial Owner(s).
The information is manually reviewed by the Company's Compliance Unit and only after an approval the business relationship may commence.
The Company collects and, if so, requested by the MROS, submits the following data on the Beneficial Owner:

- identity data of the beneficiary;
- proof of verification of the information submitted by the customer in reliable and independent sources;
- data on the ownership and management structure of the customer (legal entity).

8 REPORTING TO THE MROS

a) The Swiss defensive measures against money laundering divide the situations which have to be reported to their degree of suspicion which are the „well-founded suspicion“ and the „simple suspicion“. Depending on the degree of suspicion the Company reports their suspicion to the Money Laundering Reporting Office Switzerland (MROS) according to one of the relevant legal provisions (Art. 9, Anti Money Laundering Act, AMLA and Art. 305ter paragraph 2, Swiss Criminal Code, SCC). In addition, The SRO PolyReg has to be informed without delay about the report made and the Money Laundering Reporting Office's notifications resulting from such a report, by providing a copy of the report and notifications.

b) Internal Report. If it is identified, what is believed to be a Suspicious Monetary Operation or Transaction or Money Remittance or Money Exchange, it must immediately be reported to the Officer. This report should be made in writing and before executing the Client's instructions to affect a Monetary Operation or Transaction or Money Remittance.

c) No member of staff or personnel may disclose to the Client concerned or to a third party, the fact that an investigation is being carried out or that a SAR has been transmitted to the MROS, since such disclosure might prejudice any investigation being carried out. Furthermore, at no stage may any member of staff or personnel, tip off or warn the Client specifically about the Company's reporting obligations or that it has filed a report as this would be equivalent to alerting a suspected criminal that the Company has uncovered his illegal activity. Furthermore, such tipping off to the Client is likely to prejudice the effectiveness of any investigation or actions in regard to a Suspicious Monetary Operation or Transaction or Money Remittance.

d) Suspicious Activity Report (SAR) first case under Article 9 paragraph 1 letter a AMLA or Article 305ter paragraph 2 SCC. If the Officer finds the Monetary Operation or Transaction or Money Remittance as Suspicious Monetary Operation or Transaction or Money Remittance, the compliance Officer will submit a SAR as per Art.9, AMLA without freezing assets until the company receives further notification from MROS that the SAR has been forwarded to the prosecutor's office.

e) Suspicious Activity Report (SAR) second case under Article 9 paragraph 1 letter c n- AMLA, if the Officer finds the Monetary Operation or Transaction or Money Remittance as Suspicious Monetary Operation or Transaction or Money Remittance based on a hit of a list of terrorists, the compliance Officer will immediately freeze the assets involved for a period of five working days (Art. 10 para. 2 n-AMLA)

f) The MROS may request the Company to provide all necessary information which is needed for the MROS to carry out the verification of the Suspicious Monetary Operation or Transaction

or Money Remittance. In the latter event the Company must provide the requested information within 1 (one) business day after the receipt of the respective request of the MROS.

g) The Company, including its Employees acting in good faith, are not responsible against the Client for the non-fulfilment of any contractual obligations and for the damage caused due to the reporting and suspension of the Suspicious Monetary Operations or Transactions or Money Remittances or Money Exchange as well as for the provision of the information upon the request of the MROS.

h) Reporting forms. Due to security reasons MROS cannot receive any reports by e- mail. A general reporting form can be printed from the homepage of the Federal Office of Police and (together with the respective annexes) sent by priority "A" mail.

i) The MROS may ask for the additional information in writing or via e-mail. In the latter event the requested information must be provided in writing or via e-mail.

j) All correspondence with the MROS is to be retained, and that written records of all telephone conversations are made. Copies of all relative documentation are to be kept in the file bearing the name "Prevention of Money Laundering and Terrorist Funding".

k) The Officer is responsible for requesting guidance from the MROS on all relevant matters, if needed.

9 RECORD KEEPING

The Company must keep the following records:

Client Identification Records:

a) all records of steps taken to obtain identification records, as well as copies of evidence of the identity of the Clients as the case may be;

b) all risk assessment records as well as the Client risk profile;

c) a standard application form must be completed for every new Client as well as for the existing Client where the identification of the Client is needed under these Procedures; the filled application form must be signed off by all the Clients and prospective Clients;

d) all records related to the ongoing monitoring of the Clients.

e) Record of Monetary Operations or Transactions or Money Remittances or Money Exchange:

f) a record containing details of all Monetary Operations or Transactions undertaken in the course of an established Business Relationship or Money Remittances or Money Exchange

performed; this is to include a record of all work performed for or the services provided to the Clients;

g) Monetary Operation or Transaction or Money Remittance records are to be kept in a form which will allow a satisfactory audit trail to be completed where necessary, and which may establish a financial profile of any suspect Client;

h) records on internal and MROS Suspicious Activity Reports of Monetary Operations or Transactions or Money Remittances or Money Exchange reporting.

Other Records:

a) evidence of the training programs on ML/TF prevention whether in- house or external;

b) evidence of the proper acknowledgment of the Employees with these Procedures and their amendments as may be needed from time to time;

c) other records if required under these Procedures or the Law as well as other legal acts related to the prevention of ML/TF.

All data have to be kept for the period of 10 (ten) years as of the end of the transaction or Business Relationship with the Client.

Records may be kept both in hard copies and in soft copies. Backups of soft copies of all Monetary Operations or Transactions or Money Remittances or Money Exchange undertaken are to be taken on a regular basis at least once a month. Certain original documents or certified copies of documents obtained are to be retained in hard copies and these should never be held exclusively in electronic format.

10 TRAINING OF EMPLOYEES

The Company ensures that the members of staff, whose work duties concern the application of AML measures, have necessary qualifications and knowledge in the area of ML and TF prevention for carrying out their functions (duties) and ensures the development of its staff members' knowledge, competence and professional development.

All staff and kept personnel, whose duties include the handling of Clients' business, are to be adequately trained with respect to the procedures and the provisions of the Law, the relevant regulations and the relevant provisions in the Criminal Code of the Swiss Confederation.

The Company as an employer is required to carry out training and introduce the Procedures to all Employees before starting employment. The Company must provide inter alia, information on the obligations of the Procedures, the modern methods of ML and TF, and the risks involved, the requirements for the protection of personal data, the identification of actions relating to possible ML or TF, and instructions for action to be taken in such situations.

The level of training provided to individuals is to be appropriate to their role and seniority within the Company. In any case all Employees must have the proper training on ML/TF prevention prior to the commencement of their duties at the Company which involve the ML/TF risk.

The Officer is responsible for the proper performance of the duties related to the training of the Employees. The Officer may appoint other persons who will undertake all necessary measures for the proper training of the Employees.
Annual PolyReg training is mandatory for all staff involved in compliance activity of the Company.

Control information

Policy Number:	2023-01
Title:	Client Due Diligence and Anti-Money Laundering Policy
Policy Approver:	Director and Compliance Unit
Policy Owner:	Head of Compliance
Policy Adjustments:	Executive Management
Policy Administration:	Head of Compliance
Version:	1.0
Addressees:	All Employees
Effective from:	16 February 2023
Replaces Policy of:	None
Revision Term:	First: one year following implementation, thereafter every two years

11 ANNEX I

Transaction amount per Year	Low Risk	Medium Risk	High Risk
0 – 4'999 CHF	• ID • Sanctions screening*	• ID • Sanctions screening*	• ID • Sanctions screening* • EDD form
5'000 – 9'999 CHF	• EDD form	• EDD form **Risk-based / Case by case approach**** - Proof of address - Proof of funds - Acc. to policy	• EDD form **Risk-based / Case by case approach**** - Proof of address - Proof of funds - Acc. to policy
10'000 – 29'999 CHF	• In case of transaction exceeding 5'000 CHF / month -> Source of fund	• In case of transaction exceeding 5'000 CHF / month -> Source of fund	• Full KYC - Proof of Domicile address - Proof of income
Over 30'000 CHF	• Full KYC		

**Make sure the Sanction Screening is done via the payment system automatically or manually.*

*** The confirmation of source of funds (SOF) can be requested at any time depending of provided information.*

High risk Transactions	Method
- Unusual transaction - Destination of transaction is to a "high risk" or non-cooperative country - Funds greater than 100'000 CHF (at once or over a time period). - In regards to money or asset transfers one or more transactions, which appear interlinked, amount to or exceed a sum of CHF 5'000.	- Case by case approach and request for additional documentation can be proceeded - EDD

12 ANNEX II – LIST OF COUNTRIES CATEGORIES

Countries requiring case by case decision approach and considered as High Risk Transactions

#	Prohibited countries by FATF	#	OFAC, EU sanctions
1	North Korea (DPRK)	1	Afghanistan
2	Iran	2	Bosnia and Hercegovina
#	Jurisdictions under Increased Monitoring by FATF (High risk countries)	3	Belarus
1	Albania	4	Myanmar (Birma)
2	Barbados	5	Central African Republic
3	Burkina Faso	6	Cuba
4	Cambodia	7	Democratic Republic of the Congo
5	Cayman Islands	8	Hong Kong
6	Haiti	9	Iran
7	Jamaica	10	Iraq
8	Jordan	11	Lebanon
9	Mali	12	Libya
10	Malta	13	Nicaragua
11	Myanmar	14	North Korea
12	Nicaragua	15	Russian Federation
13	Pakistan	16	Somalia
14	Panama	17	South Sudan
15	South Sudan	18	Syria
16	Syria	19	Ukraine
17	Uganda	20	Venezuela
18	Yemen	21	Yemen
		22	Zimbabwe
		23	Crymea (Ukraine)
		24	Donetsk & Lugansk (Ukraine)