Skyindex AML/KYC Policy

Last updated: August 14, 2019

1. Company Policy

1.1 Skyindex Int OU (the Company) has set out this anti-money laundering (AML) policy that is applicable to all staff to help prevent and detect potential money laundering or terrorist financing activity. The Company takes a zero-tolerance approach to money laundering, terrorist activity and other such financial crimes.

1.2 The Company will ensure it has appropriate policies and procedures in place to complement this AML policy, in compliance with applicable regulations, and monitoring of adherence to those policies will also take place.

1.3 All staff will be trained in AML processes and procedures for the Company and will actively participate in preventing the services of the Company from being exploited by criminals and terrorists for money laundering or terrorist financing purposes. The objectives of this and related policies are:

• ensuring the Company's compliance with all applicable laws, statutory instruments of regulation, and requirements of the Company's supervisory body;

• protecting the Company and its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements;

• preserving the good name of the Company against the risk of reputational damage presented by implication in money laundering and terrorist financing activities;

• making a positive contribution to the fight against crime and terrorism.

1.4 To achieve these objectives, it is the policy of this Company that:

• every member of staff shall meet their personal obligations as appropriate to their role and position in the Company

• neither commercial considerations nor a sense of loyalty to clients shall be permitted to take precedence over the Company's anti-money laundering commitment

• the Company shall appoint a Money Laundering Reporting Officer (MLRO) and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointment;

• the Company shall have anti-money laundering policies and procedures outlining the positive actions to be taken by staff during their work, and the MLRO shall keep these under review to ensure their continuing appropriateness.

1.5 Failure to comply with the AML and associated policies could result in disciplinary proceedings which could ultimately lead to dismissal.

1.6 The above list is not exhaustive but helps set out the overall AML framework for the Company.

1.7 The Company is implementing internal controls throughout its operations designed to reduce risks of money laundering, including designating a person responsible for AML compliance. The Company performs know your customer ("KYC") procedures on all token sale purchasers.

2. Money Laundering & Terrorist Financing

2.1 Money Laundering is the process of disguising the origin of the proceeds of crime. Terrorist financing provides funds for terrorist activity. The use of products and services by money launderers and terrorists exposes the Company to significant criminal, regulatory and reputational risk.

2.2 This policy is designed to provide direction to staff on the approach and management of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) within the Company. This policy supports management's objective of mitigating the following risks:

• Money laundering;

• Terrorist financing;

• Sanctions;

• Politically exposed persons (PEPs);

• Legal and regulatory risk.

2.3 This policy applies to all individuals working at all levels within the Company, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term workers, casual and agency staff, all of whom are collectively referred to as 'staff' in this document.

2.4 The Company's MLRO will provide direction to, and oversight of, the AML and CTF strategy as well as apply a risk-based approach across the business.

2.5 The Company will enforce a strict anti-money laundering policy with zero tolerance for money laundering or terrorist financing activities and ensure it knows who its customers are and also who it is going into business with. Such activity is more commonly known as due diligence / Know Your Customer (KYC) and Know Your Business (KYB). The Company has set out robust processes and procedures to help meet these requirements.

2.6 Money Laundering

2.6.1 There are three broad groups of offences related to money laundering that the Company must avoid committing. These are:

• knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;

• failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or terrorist

financing; and

• tipping off, or prejudicing an investigation.

2.6.2 Staff will be trained in AML awareness and how to spot potentially suspicious activity.

2.7 Terrorist Financing

2.7.1 There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organized criminal activity. However, there are two major differences between terrorist property and criminal property. More generally:

• often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property;

• terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

2.7.2 The Company will ensure its staff are well versed in AML awareness and the underlying policies and procedures allowing the Company to demonstrate compliance with applicable rules and regulations in this aspect.

3. AML Risk Assessment

3.1 The Company will adopt a risk-based approach to managing the risks presented by the business, taking into account legislation and industry guidance as applicable.

3.2 The MLRO is responsible for ensuring an AML risk assessment is completed and regularly reviewed. The risks assessed should help determine the strength of the Company's policies and procedures and control systems in place to help prevent and detect such money laundering or terrorist financing activity.

3.3 The risk-based approach takes the most cost effective and proportionate way to manage and mitigate money laundering and terrorist financing risks. The MLRO will assess the money laundering and terrorist risks presented by:

• Customer risk – specific categories of customers and the resulting business relationships

• Payment risk – payment methods offered and the degree to which their specific characteristics are vulnerable to ML/TF threats

• Geographical risk – the risks posed by geographical factors

• Product risk – products offered and the degree to which their specific characteristics may be attractive for money laundering or financing terrorism

• Supplier / 3rd party Risk -risks of onboarding new clients / suppliers and not understanding who owns the business or considering other AML risks

• Technological Risk – risks with technology used by the company / how susceptible is it to money laundering or terrorist financing?

• Employee Risk – the risks posed by employees of the company

• Regulatory Risk – the risks of non-compliance with license and regulatory

frameworks and the risk of penalties to the company and individuals.

3.4 The MLRO will:

• Design and implement controls to manage and mitigate those risks;

• Monitor and seek to improve the operation of these controls; and

• Record what has been done for audit and evidence purposes.

3.5 The Company recognizes that risks change over time and will continually and regularly update its risk management procedures as part of its overall risk management framework.

4. MLRO Role and Responsibilities

4.1 The Company will designate a senior individual to be the Money Laundering Reporting Officer (MLRO) as required by the Money Laundering Regulations. The MLRO will have overall responsibility for the establishment and maintenance of the Company's AML/CTF framework and underlying systems and controls and will report to the CEO.

4.2 The Company will ensure that the MLRO is of sufficient seniority within the Company and has the relevant experience and understanding of AML/CTF to carry out their duties. The Company will fully support and ensure the MLRO has resources available for their role and will provide ongoing support and development for the MLRO.

4.3 The MLRO, with the support of the Board, is responsible for ensuring that the Company meets its AML compliance requirements in accordance with applicable legislation. The MLRO will oversee the AML systems and controls and ensure they are fit for purpose. The main activities of the MLRO comprise, but are not limited to, the following:

• oversight of all aspects of the company's AML and CTF activities;

• focal point for all activities within the company relating to AML and CTF;

• provision of AML training to all staff

• receiving all internal suspicious activity reports and, where deemed applicable, reporting to relevant authorities on the same;

• be the focal point for law enforcement and other regulatory bodies;

• establishing the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice;

• supporting and coordinating senior management focus on managing the money laundering/terrorist financing risk in individual business areas; and

• advising the business on new products / processes from an AML perspective.

4.4 The MLRO is also required to produce reports for Board meetings including, but not limited to, the following items:

• Confirmation that adequate customer due diligence information is being collected and that ongoing monitoring is taking place;

• Summary data relating to complex or unusual transactions;

• Number of internal consents / Suspicious Activity Reports (SARs) received from staff members;

• Number of SARs sent externally;

• Information on status of staff training within the company;

• Confirmation that all business records have been properly stored and are retained according to regulatory requirements;

• Changes in the law/operating environment which do or might impact the business;

• Changes in the risk matrix affecting the business; and

• Contacts with the regulator.

5 Training

5.1 All employees will be made aware, through the annual compulsory training

programme, of:

• The risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation;

• The identity and responsibilities of the Company's nominated officer (the MLRO);

• The Company's procedures in how to recognise and deal with potential money laundering or terrorist financing suspicious transactions or activity.

5.2 Staff training on anti-money laundering and counter terrorist financing will be carried out at least annually for all staff, and details will be recorded.

6. Sanctions and PEPs Screening

6.1 The Company makes use of an external service provider to screen customers against recognised Sanctions Lists and Politically Exposed Persons (PEPs) lists. Individuals will be screened on on-going basis (monthly) as well as on initial registration.

6.2 Sanctions Lists

6.2.1 The Company will take all required steps to ensure that all customers with whom a

business relationship is established are screened against relevant notices such as:

• the Office of Foreign Assets Control (OFAC)

• European Union sanctions (EU)

• United Nations sanctions (UN)

6.2.2 Information leading to "fuzzy matches" will be investigated further, for example where the match was related to a name which can be deemed as popular, and this will be compared against the other information that is collected at point of registration. The full evaluation of the customers data will provide a result.

6.2.3 Any confirmed matches to sanctions lists will be declined or closed, and the necessary reports will be made.

6.3 PEPs Screening

6.3.1 The Company will also screen customers against PEP lists that will help to structure information about PEPs.

6.3.2 The term 'politically exposed persons' (PEPs) refers to people who hold high public office. The current regime, as per the Money Laundering Regulations, requires firms to apply extra measures, called "enhanced due diligence" when dealing with those who are PEPs in a state other than the Republic of Estonia, as well as family members or close associates of those PEPs

6.3.3 The company must have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is— (a) a politically exposed person (a "PEP"), or (b) a family member or a known close associate of a PEP, and to manage the enhanced risks arising from the relevant person's relationship with such a customer.

6.3.4 Examples of prominent public functions include:

(a) heads of state, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

d) members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, charges d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;

(h) directors, deputy directors and members of the board or equivalent function of an international organization;

6.3.5 Any match, or possible match to a PEP requires the MLRO's approval and or further advice before allowing the customer to have an account with the Company. Should approval be granted for a PEP, enhanced due diligence may be required (such as additional documentation) but all PEPs will also be subject to ongoing monitoring of their account activity. This is undertaken on at least a monthly basis to ensure the customer's account is operating as expected and there are no sudden changes to account activity and / or behaviour.

7. Suspicious Activity Reporting

7.1 As a regulated company, there are various regulations that need to be complied with and the company (through its MLRO) has an obligation to report suspicious activity to the relevant financial intelligent agency. Failure to act on or report suspicions where there are reasonable grounds to suspect criminality, can be an offence under current legislation.

7.2 Staff are reminded of their obligations through training and refresher training and by following their obligations are helping the company protect itself against the risk of money laundering and terrorist financing and helping it comply with its legal obligations.

7.3 All staff must report suspicions as soon as possible following the procedures set out in the Reporting Suspicious Activity Policy. To be able to report, staff must have reasonable grounds to suspect that the activity or transaction may involve proceeds of crime and or relate to terrorist financing AND have followed procedures, gathered facts as much as possible and determined there are still reasonable grounds for suspicion.

8. Tipping Off

8.1. Under the money laundering regulations, 'tipping off' is an offence. Once an internal or external suspicious activity report has been made, it is an offence for anyone to release information to any other person which is likely to prejudice a current or proposed law enforcement investigation (in particular tipping off the actual person who is the subject of the suspicion).

8.2 Tipping Off risks become real once a suspicious activity report has been made to the MLRO and where the MLRO agrees with the underlying suspicion and submits a report. All communication between staff and the customer(s) from that point on needs to be handled with care, the MLRO will provide advice as to how to handle such situations.

8.3 To help mitigate the risk of tipping off, staff must not place any comment or reference on the customer's account related to their own suspicion or whether they have sent a suspicious activity report to the MLRO.

9. Sending SARs to the MLRO

9.1 The process for sending a SAR to the MLRO is shown below:

• Simply send an email from your personal work email address to

compliance@getskyindex.com with "SAR submission" as the subject line

• In the email provide the customer's name and any reference to the transaction / amount or email or other activity that has made you suspicious;

• Provide system references where applicable;

• Please set out a brief explanation of your reason for suspicion in the email;

• You will receive an acknowledgement of your email from the MLRO who will then review your suspicion and determine how best to proceed (including advice on how to proceed with the customer) and / or whether to submit a SAR to the NCA; and

• If your suspicion relates to a third party / supplier, set out the details of the third party / supplier and reasons why you believe their activity has made you suspicious.

9.2 Examples of emails you may send to Compliance when submitting your SAR:

9.2.1 Example 1 "Customer xxxxx, transaction reference yyyy for $100 has loaded his account with one payment method and tried to withdraw this to another method very quickly without any use. Customer's account is currently frozen".

9.2.2 Example 2 "Customer PPPP has asked to change his bank details asap as the authorities are on to him – see email reference 99999. Customer's account is currently frozen".

10. Record Keeping

10.1 The Company will principally retain the following records from an AML perspective:

• Records of customer screening (PEPs & Sanctions);

• Copies of, or references to, the evidence obtained of a customer's identity for five years after the end of the customer relationship;

• Details of customer transactions for five years from the date of the relevant transaction;

• Records of all AML/CTF training delivered;

• Details of actions taken in respect of internal and external suspicion reports;

• Details of information considered by the MLRO or his nominee in respect of an internal report where no external report is made.

11. KYC Policies and Procedures

11. 1. Purchaser Identification (Know Your Customer). The Company collects identifying information on each purchaser in its token sale. The Company shall collect the following information about each purchaser:

A) Individuals

Full Name

Wallet Address

Telephone

Email address

Residential Address

Copy (front and back) of ID Data collected from ID:

Date of birth, Nationality,

ID scan

Personal photograph (with ID in Hand) A Description of Source of Funds

PEP checks

B) Companies

Summary of information requested/gathered

Company Name

Wallet Address

Company Address

Description of Business Activities

Government-issued business registration number or tax identification number

Copy of a recent trade register extract or similar document

Authorised Representative, compare Individual of KYC process

Even after KYC approval the Company can do additional checks and ask for further documents.

2. Contributor Eligibility. The Company shall not accept purchasers (individuals or entities) who are not at least eighteen (18) years of age or purchasers from the following jurisdictions (the “Prohibited Purchasers”):

-United States - Individuals or entities from or residing in the United States, including American Samoa, Guam, Northern Mariana Islands, Puerto Rico, U.S. Virgin Islands, or any entity organized or incorporated under the laws of the United States. U.S. citizens living abroad may also be deemed "U.S. Persons" under certain rules.

The Company explicitly prohibits the Prohibited Purchasers in its Terms and Conditions (the “T&C”). Any purchasers that purchase tokens in violation of the T&C shall be deemed invalid and such purchasers shall have their purchase amount returned to them at their expense.