KYC, AMLA & CFT

1. INTRODUCTION

1.1 Prelude

Money laundering and terrorism financing (ML/FT) continues to be a plague to the global financial system and has been recognised as a crime worldwide. Through laundering illicit proceeds, ML/FT corrodes the financial market and ultimately affect the political, economic and social stability of a country. Therefore, combating ML/FT has, in recent year, become a global effort for most countries where effective measures and approaches are adopted to mitigate the ML/FT risks.

Any financial institution regulated and operated in Lithuania is bound to comply with all AML/CFT regulations and guidelines to prevent themselves from being used as a vehicle by the criminals to launder illegal proceeds. This is pertinent to promote and uphold the integrity and transparency of the financial market.

1.2 Objective

This Anti-Money Laundering and Counter Financing Terrorism Manual ("AML Manual") is adopted to ensure that the Exchange complies with the rules and regulations set out in:

- the Czech Republic Money Laundering and Terrorist Financing Prevention Act;
- the Czech Republic International Sanctions Act (ISA);
- FAO general guidelines regarding measures against money laundering, terrorist financing and regarding implementation of international sanctions;
- DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (AMLD5).

With an objective to ensure all members of Unicoin Digital Capital Exchange (UDCX) understands and complies with the requirements and obligations imposed on them under the law.

1.3 Definitions

The Money Laundering (ML) means the concealment of the origins of illicit funds through their introduction into the legal economic system and transactions that appear to be legitimate. There are three recognized stages in the money laundering process:

- placement, which involves placing the proceeds of crime into the financial system;
- layering, which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds;
- integration, which involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

The Terrorist Financing (TF) means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism in the meaning of applicable legislation.

Sanctions mean an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the common foreign and security Policy of the European Union. Sanctions include:

- international sanctions which are imposed with regard to a state, territory, territorial unit, regime, organization, association, group or person by a resolution of the United Nations Security Council, a decision of the Council of the European Union or any other legislation imposing obligations on Czech Republic;
- sanctions of the Government of the Republic of Czech Republic which is a tool of foreign policy which may be imposed in addition to the objectives specified in previous clause in order to protect the security or interests of Czech Republic.

International sanctions may ban the entry of a subject of an international sanction in the state, restrict international trade and international transactions, and impose other prohibitions or obligations.

The subject of Sanctions is any natural or legal person, entity, or body, designated in the legal act imposing or implementing Sanctions, with regard to which the Sanctions apply.

The Customer means a natural person or a legal entity which has the business relationship with the Exchange or a natural person or legal entity with which the Exchange enters into the occasional transaction.

The Beneficial Owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or exercises control in another manner over a transaction, act, action, operation or step or over another person and in whose interests or for whose benefit or

on whose account a transaction or act, action, operation or step is made. In the case of a legal entity, the beneficial owner is a natural person whose direct or indirect holding, or the sum of all direct and indirect holdings in the legal person, exceeds 25 percent, including holdings in the form of shares or other forms of bearer.

MLRO means Money Laundering Reporting Officer, who is appointed to the Exchange as a compliance officer.

The Employee means the Exchange´s employee, including persons which are involved in application of these Guidelines in the Exchange.

The Management Board means management board of the Exchange.

The Business Relationship means a relationship that is established upon conclusion of a long-term contract by the Exchange in economic or professional activities for the purpose of provision of a service or distribution thereof in another manner or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the Exchange repeatedly makes separate transactions in the course of economic or professional activities while providing a service.

The Occasional Transaction means the transaction performed by the Exchange in the course of economic or professional activities for the purpose of provision of a service or sale of goods or distribution thereof in another manner to the Customer outside the course of an established business relationship.

Virtual currency means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive.

PEP means a natural person who performs or has performed prominent public functions and with regard to whom related risks remain.

1.4 Purpose of This Policy

a. This policy aims at assisting all members of UDCX to:-

   I. (Understand and comply with their obligations under the AML/CFT laws and regulations;
   II. Understand and able to apply "Know your Client" (KYC), Customer Due Diligence (CDD) and Risk- based Approach (RBA) knowledge in the client identification and verification process; and
   III. Create an effective compliance culture and high ethic within the organization

b. It is expressly stated that this manual provides the general and minimum criteria to be adhered by its members under normal circumstances. It is the responsibility of the management to establish additional AML/CFT control as well as upgrading this manual where necessary depending on the circumstances.

1.5 Exchange Compliance Culture

a. UDCX recognizes its AML/CFT roles and is committed to comply and implement the AML/CFT laws and regulations in its business dealings.
b. In this regard, UDCX has developed its AML manual based on the requirements set by the Financial Analytical Office (FAO) as well as some international agencies such as the FATF. This is pertinent in deterring criminals from abusing its services to launder illicit proceeds. In addition, UDCX recognizes the importance of continuous vigilance in developing a robust AML/CFT framework and full cooperation with the authorities in the implementation of AML/CFT laws and regulations to achieve its purposes.
c. UDCX and its subsidiaries and branches shall make all endeavours to understand their responsibilities under this AML Manual and comply with the same in order to build an excellent compliance culture within the organisation.
d. With these basic tenets in place, Unicorn may conduct its business with high compliance ethics and integrity which are essential to prevent from it from being abused by criminals as an ML/FT vehicle.

2. RISK BASED APPROACH (RBA)

2.1 UDCX adopts risk-based approach (RBA) in its client on-boarding, which is a measure to identify, understand and assess the risk profile of the client and mitigate the risk identified with appropriate risk mitigation methods.

2.2 The key features of RBA involve the following:

a. Risk Profiling: UDCX shall collect the client's profile and consider the risks by taking into account the following:

(i) Customer risk

(ii) occupation of the client

(iii) nationality of the client

(iv) PEP identity

(v) Geographical risk

(a) origin of the client

(b) place of business

(vi) Product and services risk

(vii) type of products and services acquired by the client

(viii) Delivery channels

(a) Face-to-face relationship

(b) Non face-to-face relationship

b. Risk Assessment: UDCX shall assess the client's risk by doing the following:

(i) refer to the client's profile earlier collected and consider all the risks identified;

(ii) assess and determine the level of overall risk (low, medium or high) according to its risk appetite;

(iii) determine the appropriate risk mitigation method against the risk identified; and

(iv) document the risk assessment and findings for on-going monitoring purpose.

c. Risk Mitigation: Where a higher risk client is identified, UDCX shall take appropriate mitigating method to mitigate and manage the risk by conducting enhanced due diligence (EDD) on the client.

3. Customer Due Diligence (CDD)

3.1 Know Your Client (KYC)

It is important for UDCX to apply the principle of "Know Your Client" (KYC) in its business dealings. In order to know each of the client, UDCX shall conduct Customer Due Diligence (CDD) on its client.

3.2 Timing of Identification and Verification

UDCX is required to conduct identification and verification on its client before, during and after the establishment of the business relationship.

3.3 Circumstances of Identification and Verification

a. UDCX shall take steps to understand their client on the below circumstances:
    i. during the establishment of a business relationship;
    ii. any changes of the client's profile or CDD;
    iii. there is suspicion or doubt in the transaction; and
    iv. on a case-by-case basis as the Compliance Officer thinks fit.
b. which include the background of the client, full structure of the organisation, the ultimate beneficial owner, nature and purpose of the business, source of fund and source of wealth.
c. This can be done by conducting customer due diligence (CDD) on each client through established identification and verification process and procedure by UDCX.
d. Identification and verification of client includes the below:
    i. identify and verify the identity of the client using reliable and independent source of documents, data or information;
    ii. identify and verify the identity of a nominee or representative purporting to act on behalf of the client and further verify its authority;
    iii. identify and verify the beneficial owner and if the client is a legal entity, the ownership and control structure of the organization;
    iv. understand the nature and purpose of the business; and

v. conduct on-going monitoring on the client throughout the business relationship to ensure the transaction is consistent with UDCX's knowledge on the client, its business and risk profile as well as the source of fund

3.4 Customer Due Diligence (CDD) Requirements

a. Natural Person: When conducting CDD on a natural person, UDCX shall obtain the below:
   i. Full name;
   ii. Passport or Identification document bearing a photograph of the client;
   iii. Residential or mailing address;
   iv. Date of birth;
   v. Nationality; and
   vi. Purpose of transaction.

b. Legal Entity: Where the client is a legal entity, UDCX shall obtain the below:
   i. Name, legal form and proof of existence such as the Certificate of Incorporation or Establishment, Constitutions or other documentary proof;
   ii. Registered office address, if different, the principle place of business;
   iii. Powers that regulate and bind the client such directors' resolution; and
   iv. Name of the senior management.

c. UDCX shall take steps to ensure that it is fully satisfied with the ownership and control structure of the legal entity as well as the identity of its beneficial owner(s) by obtaining the below:
   i. Confirmation of the ultimate beneficial owner or effective controller;
   ii. Identity of the directors;
   iii. Identity of the shareholders or partners with equity interest of more than twenty-five percent (25%);
   iv. Proof of authority of a nominee or representative such as a letter of authorization or directors' resolution;
   v. Such other information or documents as may be required by the Compliance Officer from time to time.

d. Where there is an absence or there is impractical to identify any beneficial owner in a legal entity, UDCX may obtain the identity of the senior management.

e. Where there is suspicion or doubt in the process of identification and verification of a legal entity, UDCX shall take the below steps:

i. conduct a basic search or enquiry on the background of the legal entity to ensure it is not in theprocess of dissolution or liquidation or bankruptcy; and

ii. verify the authenticity of the information provided by the legal entity with relevant authorities.

4. <u>SIMPLIFIED DUE DILIGENCE (SDD)</u>

4.1 UDCX is allowed to exercise simplified due diligence (SDD) towards a lower risk client, provided such low risk classification is pursuant to the standards and guidelines issued by relevant authorities.

4.2 SDD may be applied to the following entities:

a. public listed companies or corporations listed in Lithuania;

b. foreign public listed companies which are listed on recognised exchanges and not from a high- risk jurisdiction;

c. foreign financial institutions that are not from a high-risk jurisdiction;

d. government-linked companies in Lithuania;

e. stated-owned enterprises in Lithuania;

f. Persons licensed or registered by the FAO;

4.3 It is expressly stated that SDD shall not apply in circumstances where higher risk is identified or the existence of suspicion or doubt. UDCX shall document the assessment and rationale behind such SDD decision and make available all relevant information if so requested by the authorities.

5. <u>Enhanced Due Diligence</u>

5.1 Where a client is identified with a higher risk, UDCX shall conduct enhanced due diligence (EDD) on the client by applying a higher degree of CDD to commensurate with the risk identified. EDD may include the below:

a. Obtaining additional information on the client (i.e., source of fund and source of wealth of the client, intended volume and nature of the business, etc.);

b. More regular update on the CDD of the client;

c. Inquiring on the reason for certain transactions;

d. Obtaining approval from the senior management for continuation of business relationship; and
e. Conducting more frequent on-going monitoring on the business relationship by increasing the degree and frequency of controls and selecting transactions that require further analysis.

6. Non-Face-To-Face Business Relationship

6.1 Extra vigilance shall be exercised during the establishment of a non-face-to-face business relationship through electronic devices due to the exposure of higher risk. The CDD conducted shall be as effective as a face-to-face business relationship. It is pertinent to ensure adequate monitoring and reporting measures to identify and mitigate any potential ML/FT risks.

7. Existing Clients

7.1 For existing client, UDCX is required to conduct the usual CDD on the premise of materiality and risk to ensure that the CDD is always relevant and up-to-date. In assessing the materiality and risk of an existing client, UDCX may take into account the following:
a. The nature, significance and circumstances of the transaction;
b. Any material change in the transaction or the business relationship; and
c. Inadequate or change of the client's CDD.

8. Third Party CDD Reliance

8.1 UDCX may rely on a third party to conduct CDD or to introduce business, provided that such third party is not from a high-risk jurisdiction or identified by the Government of Lithuania as having strategic AML/CFT deficiencies. However, UDCX is aware that the ultimate responsibility and accountability of CDD shall remain with UDCX.

8.2 It is important for UDCX to establish sound policies and procedures to govern the reliance on third parties particularly those from a foreign jurisdiction having strategic AML/CFT deficiencies and will expose UDCX to higher ML/FT risk.

8.3 A relationship with any third party shall also be governed by a proper instrument which specifies the rights, obligations, liabilities and expectations between each other. It is crucial to ensure that the below criteria are duly considered:

a. Integrity and reputation of the third party;
b. Adequacy of the AML/CFT framework;
c. Establishment of CDD process and procedure;
d. Record keeping undertaking;
e. Undertaking to furnish relevant information and document upon request;
f. Regulated and supervised by relevant authorities.

9. Politically Exposed Persons (PEPS)

9.1 A business relationship with a politically exposed person (PEP) tends to expose UDCX to a higher risk. This is because a PEP who holds a prominent public position may be influential and dominant enough to attract bribes and corruption by using their special position.

9.2 PEPs include the family members, i.e., parents, spouse, parents-in-law, siblings, children and relatives as well as close associates, i.e., business partners, representatives, close friends and financially independent individuals.

9.3 The Exchange shall verify the data received from the Customer by making inquiries in relevant databases or public databases or making inquiries or verifying data on the websites of the relevant supervisory authorities or institutions of the country in which the Customer has place of residence or seat. PEP must be additionally verified using Google and the local search engine of the Customer's country of origin, if any, by entering the customer's name in both Latin and local alphabet with the customer's date of birth.

9.4 At least the following persons are deemed to be PEPs:

a. head of State or head of government;
b. minister, deputy minister or assistant minister;
c. member of a legislative body;
d. member of a governing body of a political party;
e. judge of the highest court of a country;
f. auditor general or a member of the supervisory board or executive board of a central bank;
g. the Chancellor of Justice;
h. ambassador, envoy or chargé d’affaires;
i. high-ranking officer in the armed forces;

j. member of an administrative, management or supervisory body of a state-owned enterprise;

k. director, deputy director and member of a management body of an international organisation;

l. person in list of Czech Republic positions whose holders are considered politically exposed persons is established by a regulation of the minister responsible for the field;

m. person in list of positions, which is established by international organisation accredited in Czech Republic;

n. a person who, as per list published by the European Commission, is considered a performer of prominent public functions by a Member State of the European Union, the European Commission or an international organisation accredited on the territory of the European Union is deemed a politically exposed person.

9.5 When a PEP is identified in the establishment of a business relationship, UDCX shall exercise EDD and document the assessment and findings.

10. <u>High Risk Jurisdictions</u>

10.1 Where a client is identified to be connected with a jurisdiction identified by the FATF, other international AML bodies or the Government of Lithuania as having substantial AML/FCT deficiencies, UDCX are required to exercise EDD on such client.

10.2 Establishing a business relationship with a client connected with high risk jurisdiction will expose UDCX to further reputational and regulatory risk, therefore appropriate measures must be taken to mitigate the risk.

10.3 In addition to the EDD, UDCX may take the below measures:

a. Limiting the business relationship or financial transaction with the client connected with a high- risk jurisdiction;

b. Conducting enhanced external audit by increasing the intensity and frequency for branches and subsidiaries of UDCX located in a high-risk jurisdiction; and

c. Conducting such other measures as may be specified by the authorities from time to time.

11. On-Going Monitoring

11.1 Upon the completion of identification and verification of client and the establishment of business relationship, UDCX shall conduct on-going monitoring on its client in accordance to the risk level. This shall include the below

a. Scrutinising transactions throughout the business relationship to ensure its consistency with Uncoin's knowledge on the client and the client's business and risk profile and if necessary, the source of fund;

b. Screening transactions undertaken by the client to ensure all transactions with compromised digital assets addresses or its equivalent are identified and prohibited. A digital assets address is considered compromised if there is suspicion that it is being used for the purpose of fraud, identity theft, extorting ransom or any other crimes; and

c. Ensuring the client's CDD is relevant and up-to-date, inter alia, the high risk client.

11.2 In conducting on-going monitoring, UDCX shall consider the economic circumstances and the purpose of a transaction or business relationship which:

a. Appears unusual; and

b. Casts doubt on the legality of the transaction, especially with regard to complex and large transaction or when high risk client is involved.

11.3 The degree and frequency of on-going monitoring shall commensurate with the risk level of each client based on the RBA. Higher degree and frequency of on-going monitoring shall apply on high risk client while for lower risk client, a lower degree and frequency.

12. New Products, Services and Practices

12.1 When there is any new products, services or practices in the market such as new digital assets, electronic platforms, devices, systems, information technologies or delivery channels, Unicoin shall assess and identify its potential ML/FT risks by taking the below steps:

a. Conduct risk assessment before the adoption of such new products, services and practices;

b. Adopt appropriate measures to mitigate the potential ML/FT risks; and

c. Document the assessment and findings.

13. Management Information System (MIS)

13.1 UDCX shall establish sound management information system (MIS) in conducting the CDD. A sound MIS is crucial in providing support to an organisation with accurate and timely information in the detection of potential ML/FT risks.

13.2 It is important to ensure that the MIS commensurate with the size, nature, scale and complexity of an organisation and its ML/FT risk profile and appetite. The MIS shall be, at the minimum, able to capture information of multiple transactions over a certain period, large transactions, unusual or dubious transaction patterns, client's risk profiles, transactions exceeding a particular threshold, etc. The MIS shall also be able to aggregate the client's transactions from multiple accounts and/or different systems.

14. REPORTING OBLIGATION

14.1 The Exchange through its MLRO must report to the FAO on the activity or the circumstances that they identify in the course of economic activities and whereby:

a. the characteristics indicate the use of criminal proceeds or the commission of crimes related to this (this is primarily a report on a suspicious and unusual transaction or activity, i.e. UTR or UAR);

b. in the case of which they suspect or know or the characteristics of which indicate the commission of money laundering or related crimes (this is primarily a report on a transaction or activity whereby money laundering is suspected, i.e., STR or SAR);

c. in the case of which they suspect or know or the characteristics of which indicate the commission of terrorist financing or related crimes (this is primarily a report on a transaction or activity whereby terrorist financing is suspected, i.e., TFR);

d. in the case of which an attempt of the activity or circumstances specified in previous clauses is present.

The minimal characteristics of suspicious and unusual transactions are provided in the guidelines made by the FAO (one of annexes of these Guidelines).

14.2 The Exchange through its MLRO must report the FAO:

a. about the circumstances of refusal of establishment of the business relationship and about the termination of the business relationship on the basis of circumstances

provided in the previous chapter (primarily a suspicious and unusual transaction or activity report, i.e. UAR);

b. about each transaction that has become known whereby a pecuniary obligation of over 32 000 euros or an equal sum in another currency is performed in cash, regardless of whether the transaction is made in a single payment or in several linked payments over a period of up to one year (an amount-based report, CTR);

c. about identifying the subject of the Sanctions and the implementation of Sanctions or suspicion thereof (international sanction report, ISR).

14.3 The reports specified above must be made before the completion of the transaction if the Exchange suspects or knows that money laundering or terrorist financing or related crimes are being committed and if said circumstances are identified before the completion of the transaction. If the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede capture of the person who committed possible money laundering or terrorist financing, the transaction will be concluded and a report will be submitted the FAO thereafter. The Exchange is in contact with FAO in order to identify such circumstances.

14.4 If the necessity of abovementioned report arises, the Employee to whom became known such necessity must immediately notify the MLRO about this.

14.5 In any case (i.e. also in the situation where an activity or circumstance is identified after the completion of the transaction), the reporting obligation must be performed immediately, but not later than two working days after the identification of the activity or circumstance or the emergence of the actual suspicion (i.e. the situation where the suspicion cannot be dispelled).

14.6 The report shall be sent in accordance with the guidelines, issued by the FAO (one of annexes of these Guidelines).

14.7 Internal Reporting: Where a suspicious transaction is detected, an internal suspicious transaction report (ISTR) shall first be submitted by the staff who discovers the suspicious transaction to the Compliance Officer at the head office within a reasonable time upon which the Compliance Officer shall carefully evaluate the ISTR with all relevant information and document available. This evaluation process shall take place within a

reasonable time and shall be documented. Full cooperation shall be rendered by all members of UDCX to the Compliance Officer during the evaluation stage.

15. RECORD KEEPING

15.1 The Exchange through the person (incl. Employees, Management Board members and MLRO) who firstly receives the relevant information or documents shall register and retain:

a. all data collected within CDD measures implementation;
b. information about the circumstances of refusal of the establishment of the business relationship by the Exchange;
c. the circumstances of the refusal to establish business relationship on the initiative of the Customer if the refusal is related to the application of CDD measures by the Exchange;
d. information on all of the operations made to identify the person participating in the transaction or the Customer´s beneficial owner;
e. information if it is impossible to take the CDD measures using information technology means;
f. information on the circumstances of termination of the business relationship in connection with the impossibility of application of the CDD measures
g. each transaction date or period and a description of the contents of the transaction;
h. information serving as the basis for the reporting obligations specified above;
i. data of suspicious or unusual transactions or circumstances of which the FAO was not notified.

15.2 In addition to the abovementioned information the Exchange shall register the following data regarding a transaction:

a. upon opening an account, the account type, number, currency and significant characteristics of the securities or other property;
b. upon making a payment relating to shares, bonds or other securities, the type of the securities, the monetary value of the transaction, the currency and the account number;

c. in the case of another transaction, the transaction amount, the currency and the account number.

15.3 The data specified above shall be retained for 5 years after the expiry of the business relationship or the completion transaction. The data related to the performance of the reporting obligation must be retained for 5 years after the performance of the reporting obligation.

15.4 Documents and data must be retained in a manner that allows for exhaustive and immediate response to the queries made by the FAO or, pursuant to legislation, other supervisory authorities, investigation authorities or the court.

15.5 The Exchange implements all rules of protection of personal data upon application of the requirements arising from the applicable legislation. The Exchange is allowed to process personal data gathered upon CDD implementation only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

15.6 The Exchange deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time period.

16. <u>Combating Terrorism Financing</u>

16.1 UDCX shall maintain sanctions list which contain individuals and entities sanctioned by the United Nations Security Council (UNSC). Besides than the UN Sanctions List, UDCX shall maintain such orders as may be issued by the FAO.

16.2 UDCX shall ensure the UN Sanctions List and orders under the AMLA are always relevant and updated and easily accessible by its members.

16.3 Screening shall be performed on all new and existing clients against the UN Sanctions List and order under the AMLA and where there is a match, UDCX shall take reasonable and appropriate steps to identify and verify the match. Upon confirmation that the match is genuine, UDCX shall promptly:

a. Freeze the client's funds or block the transaction, where necessary;
b. Reject the business relationship;
c. Terminate the business relationship; and
d. File STR to the authorities.

17. <u>TRAINING OBLIGATION</u>

17.1 The Exchange ensures that its employees, its contractors and others participating in the business on a similar basis and who perform work tasks that are of importance for preventing the use of the business for money laundering or terrorist financing ('Relevant Persons') have the relevant qualifications for these work tasks. When a Relevant Person is recruited or engaged, the Relevant Person's qualifications are checked as part of the recruitment/appointment process by carrying out background checks comprising extracts from criminal records in addition to the customary taking of references, which is documented using a special standard form assessing employee suitability.

17.2 In accordance with the requirements applicable to the Exchange on ensuring the suitability of Relevant Persons, the Exchange makes sure that such persons receive appropriate training and information on an ongoing basis to be able to fulfil the Exchange's obligations in compliance with the applicable legislation. It is ensured through training that such persons are knowledgeable within the area of AML/CFT to an appropriate extent considering the person's tasks and function. The training must provide, first and foremost, information on all the most contemporary money laundering and terrorist financing methods and risks arising therefrom.

17.3 This training refers to relevant parts of the content of the applicable rules and regulations, the Exchange's risk assessment, the Exchange's Guidelines and procedures and information that should facilitate such Relevant Persons detecting suspected money laundering and terrorist financing. The training is structured on the basis of the risks identified through the risk assessment policy.

17.4 The content and frequency of the training is adapted to the person's tasks and function on issues relating to AML/CFT measures. If the Guidelines is updated or amended in some way, the content and frequency of the training is adjusted appropriately.

17.5 For new employees, the training comprises a review of the content of the applicable rules and regulations, the Exchange's risk assessment policy, these Guidelines and other relevant procedures.

17.6 The employees and the Management Board members receive training on an ongoing basis under the auspices of the MLRO in accordance with the following training plan:

a. periodicity: at least once a year for the Management Board members. At least once a year for the Exchange's employees and Relevant Person engaged.

b. scope: review of applicable rules and regulations, the Exchange's Guidelines and other relevant procedures. Specific information relating to new/updated features in the applicable rules and regulations. Report and exchange of experience relating to transactions reviewed since the previous training.

17.7 In addition to the above, Relevant Persons are kept informed on an ongoing basis about new trends, patterns and methods and are provided with other information relevant to the prevention of money laundering and terrorist financing.

17.8 The training held is to be documented electronically and confirmed with the Relevant Person signature. This documentation should include the content of the training, names of participants and date of the training.