

Anti-Money Laundering and Counter Financing of Terrorism Policies and Procedures

Luxsoft N.V.

CONFIDENTIAL



(SMES) Solutions for Management and Employment Support N.V.

Managing Director

14.11.2025

This Document is intended only for the following users:

<u>User Types</u>
General Users (All Employees)

Version Control:

<u>Document Version</u>	<u>Document Author</u>	<u>Approved By</u>	<u>Document Purpose</u>	<u>Release Date</u>
1.0	Mr. Igor Basistii – MLRO	Mr. Anatolii Snehirov – UBO	Initial Release	12/11/2025

Table of Contents

1.	Objectives.....	4
2.	Policy Statement.....	4
3.	General Definitions.....	4
4.	Introduction.....	7
4.1.	Stages of money laundering.....	8
4.2.	Placement.....	8
4.3.	Layering.....	9
4.4.	Integration.....	9
4.5.	Terrorist Financing.....	9
4.6.	Financing of Proliferation.....	10
5.	Responsibilities.....	10
6.	AML Policies and Procedures.....	11
6.1.	AML Detection.....	11
6.2.	Implement and clearly communicate policies and procedures to staff.....	12
6.3.	Risk Based Approach.....	12
6.4.	Internal Controls – Implementation of the Risk Based Approach.....	14
6.5.	Dynamic Risk Management.....	14
6.6.	Customer Acceptance Policy.....	15
6.6.1.	Failure or refusal to submit information.....	15
6.6.2.	General Principles of the CAP.....	16
6.6.3.	Criteria for Accepting New Clients (based on their respective risk).....	17
6.6.4.	Low Risk Clients.....	17
6.6.5.	Medium Risk Clients.....	17
6.6.6.	High Risk Clients.....	17
	Player Registration.....	18
	Email Verification.....	18
6.7.	Customer Risk Level Breakdown.....	18
6.8.	Customer Due Diligence.....	19
6.9.	Player Verification Procedure.....	25

6.10. Applied Due Diligence Measures and Account controls breakdown.....	26
6.11. Protection of Minors and Responsible Gaming.....	31
6.12. Politically Exposed Persons.....	32
6.13. Ongoing Risk Assessment – Advanced.....	36
6.14. Record Keeping and Monitoring.....	42
6.14.1. General.....	42
6.14.2. Format of Records.....	43
6.14.3. Certification and language of documents.....	43
6.14.4. AML/CFT Audits.....	43
6.15. On-going Monitoring Process.....	44
6.15.1. General.....	44
6.15.2. Procedures.....	44
6.15.3. Timeframes.....	45
6.15.4. Payout Management Procedure.....	45
6.15.5. Reporting to the CGA.....	48
6.16. Dormant Accounts.....	48
6.17. Technical Compliance.....	48
6.18. Licensing Compliance.....	49
7. Suspicious Activity Reporting.....	49
7.1. Knowledge.....	50
7.2. Suspicious Transactions.....	50
7.3. MLRO's Report to the FIU.....	52
7.4. Submission of Information to the FIU.....	52
8. Training.....	56
8.1. Employees' obligations.....	56
8.2. Employees' Education and Training.....	57
8.3. MLRO Education and Training Program.....	57
9. Agents/Intermediaries.....	58
Annex A: List of Prohibited Countries.....	59
Annex B: EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING.....	61
A. MONEY LAUNDERING.....	61
B. TERRORIST FINANCING.....	65

1. Objectives

The aim of this document is to define the manner in which the settlement process towards players is carried out, the procedure to be utilized for verifying player identity, and the means by which all transactions are monitored to avoid fraudulent activities.

2. Policy Statement

Luxsoft N.V. is committed to preventing its services from being used for money laundering, terrorist financing, or proliferation financing, in full compliance with the National Ordinance on Games of Chance (LOK), Curaçao laws, and international AML/CFT standards. This policy applies to all employees, departments, and operations under the company's B2C gaming license.

3. General Definitions

For the purposes of this Manual, unless the context shall prescribe otherwise:

- **“Advisory Authority”** means the Advisory Authority for Combating Money Laundering and Terrorist Financing.
- **“Beneficial Owner”** means the natural person or natural persons, who ultimately owns or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted.
- **“Business Relationship”** means a business, professional or commercial relationship which is connected with the professional services offered by the Company and which was expected, at the time when the contact was established, to have an element of duration.
- **“CDD”** – customer due diligence.
- **“CFATF”** - means the Caribbean Financial Action Task Force.

- **“Client”** means any legal or physical person aiming to conclude a Business Relationship or conduct a single transaction with the Company.
- **“Company”** means Luxsoft N.V., a company which is duly incorporated under the Laws of Curaçao, with registered No. 166297, having its registered address at Dr. H. Fergusonweg 1, Curaçao, and its related companies and entities.
- **“Curaçao Gaming Authority (CGA)”** means the authority established under the Compliance Ordinance on Games of Chance, responsible for issuing and managing gaming licenses in Curaçao, enforcement, AML/CFT supervision, and operational compliance oversight in the gaming sector in Curaçao, under the National Ordinance on Games of Chance (LOK).
- **“EDD”** – enhanced due diligence.
- **“European Economic Area (EEA)”** means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.
- **“EU Directive”** means the Directive (EU) 2023/1544 of the European Parliament and of the Council of 18 October 2023 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending previous Directive (EU) 2018/1673.
- **“FATF”** – means the Financial Action Task Force.
- **“FIU”** – means the Financial Intelligence Unit of Curaçao.
- **“Law”** means any Laws and Acts legally enacted from time to time in Curaçao, or which

are applicable and enforceable in Curaçao.

- **“Manual”** means the Anti-Money Laundering and Counter Financing of Terrorism Policies and Procedures.
- **“Money Laundering and Terrorist Financing”** or **“ML/TF”** means the money laundering offences and terrorist financing offences defined in the Law.
- **“Occasional Transaction”** means any transaction other than a transaction carried out in the course of an established Business Relationship formed by a person acting in the course of financial or other business.
- **“Politically Exposed Persons (PEPs)”** means the natural persons who have their place of residence in Curaçao or any other country and who are or have been entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons (see also section 6.12).
- **“PEP Status Screening”** means the process of identifying and verifying whether individuals involved in transactions or business relationships qualify as Politically Exposed Persons (PEPs), as defined under Curaçao’s anti-money laundering and counter-terrorism financing regulations. This includes screening clients, beneficial owners, and relevant parties against criteria for domestic, foreign, or international organization PEPs, as outlined in the National Ordinance on Identification when Rendering Financial Services and related guidelines. The screening is conducted during onboarding, ongoing monitoring, and transaction reviews to assess heightened risks associated with PEPs, requiring enhanced due diligence measures and, where applicable, reporting to the Financial Intelligence Unit (FIU-Curaçao) in accordance with Curaçao’s legal framework.
- **“Sanctions Screening”** means the process of verifying whether individuals, legal entities, or organizations involved in transactions are listed on national or international sanctions lists, as required under Curaçao’s anti-money laundering, counter-terrorism

financing, and counter-proliferation financing laws. This includes checking consolidated lists issued by the United Nations Security Council, the European Union, and Curaçao authorities, as well as conducting customer and transaction due diligence to identify, freeze, and report any matches or suspicious activities to the Financial Intelligence Unit (FIU-Curaçao) in accordance with the National Ordinance on the Reporting of Unusual Transactions.

- **“Tipping-Off”** refers to the act of informing a client or third party that a suspicious transaction report (STR) has been or will be filed with the FIU, which is prohibited under Curaçao law.
- **“KYC”** for Know Your Customer
- **“Virtual Assets (VAs)”** refer to digital representations of value that can be digitally traded or transferred, such as cryptocurrencies.
- **“Virtual Asset Service Providers (VASPs)”** include entities that facilitate the exchange, transfer, or storage of VAs.

4. Introduction

The AML/CFT policy document shall indicate and define the company’s policies and procedures in place intended to prevent its products and/or services being used for ML/TF purposes. This document shall set the standard to be followed by the company, its officers and employees, the measures and controls in place and the internal practices to follow. The AML/CFT manual shall be reviewed at least on a yearly basis to determine if any updates and/or amendments are required. The frequency of such updates can be less should there be any regulatory change or change in the policies and procedures to be applied due to any change in the risks faced by the company or due to any changes in the assessment of certain risk factors arising out of publications made by the FIU, FATF, National Risk-Assessments and/or supra-national Risk Assessments. It shall be the MLRO’s responsibility to ensure that this document is reviewed and updated if and when required. Any updates and/or changes made to this document shall be presented to the

board of directors who shall review and approved such changes.

Luxsoft N.V. is in the process of obtaining a B2C license issued by the Curaçao Gaming Authority (CGA) in accordance with the National Ordinance on Games of Chance (LOK). The company complies with all applicable laws and regulations in Curaçao, including those enforced by the Curaçao Gaming Authority (CGA) for AML/CFT and operational oversight.

4.1. Stages of money laundering

The company strives to ensure that all possible efforts are undertaken to prevent money laundering or the funding of terrorism and actively act to curtail such illicit activity. The company complies with the EU Sixth Anti-Money Laundering Directive (Directive (EU) 2023/1544), EU Fifth Anti-Money Laundering Directive (Directive (EU) 2018/843) and Funding of Terrorism Regulation SL373.01, Prevention of Money Laundering Act 373, the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance on Identification when Rendering Services (NOIS), and any other applicable laws and regulations in Curaçao and the EU.

Money laundering is an offence by which money derived from criminal activity is passed through a series of processes to disguise the ownership and management of such revenue which therefore cannot be traced back to the underlying crime. The process of money laundering makes such funds appear to have been generated from legitimate sources of business.

The stages of money laundering are as follows:

- I. Placement
- II. Layering
- III. Integration

4.2. Placement

Placement is the stage where the money is introduced into the financial system, the funds at this stage are still illegitimate and the launderer will try to incorporate and place the money derived from illicit activity into the system to start the process of money laundering. At this stage it is very important to understand where the money originates from, as the

person with the intention of committing such act will need to obfuscate any link of the funds with criminal activity without attracting any attention.

There are a number of methods for a launderer to perform the placement stage including, cash deposit cheques, traveler's cheques, gambling, loan repayments, life insurance policies, deposits in an amount of less than 10,000, mixing legitimate with illegitimate funds and asset purchasing.

4.3. Layering

At this stage the funds have managed to be deposited in the financial institution it is at this point layering is used through complex structures directed to lose all trace of the money and remove any trace of its origination from the proceed of a crime. This may happen by conducting transactions to different jurisdictions. This process is intended to ensure that the funds are as far removed as possible from the proceeds of a crime.

It is important to prevent such an event by transaction by ensuring staff are equipped to ask the right questions whilst avoiding alerting the customer of any suspicion. Tipping of a money launder can have severe penalties, so all staff are regularly trained in how to detect at which point a transaction is out of their comfort zone and how to interact in a way that would not alert the individual making the transaction of any suspicion.

4.4. Integration

At this stage, the money derived from criminal activity has been made legitimate and placed once again into the financial system as legitimate funds. At this stage, the launderer has been successful in laundering the funds.

4.5. Terrorist Financing

When dealing with the issue of terrorist financing, an important aspect is that the money does not necessarily have to be derived from criminal activity. The funds may be legitimate. It is not a case of disguising the source of the funds but simply the intentional transfer of funds from A to B with the intention of the receiver using those funds to support terrorist activity.

The intent and the scope of such acts are different and differ from case to case, but the process used for the funding of terrorism can be fairly similar to those methods used for

money laundering.

Current legislation enforces Customer Due Diligence on transactions and having this process in place has made such activity harder for those intent on laundering money generated from illegal activities. It is of utmost importance the company that the policies and procedures are structured in a way that they ensure compliance with regulators and legal frameworks, ensuring that the company is not an attractive vehicle for the purpose of terrorist financing.

The Firm's AML policies, procedures and internal controls are designed to ensure compliance with all applicable legislations and best practice procedures. Policy is reviewed and updated on a regular basis to ensure all applicable procedures and internal controls are up to date to account for both changes in regulation and internal changes that could present new risk factors.

4.6. Financing of Proliferation

The Company shall take measures to prevent and detect the financing of proliferation of weapons of mass destruction, in line with the relevant UN Security Council Resolutions, Kingdom Sanctions Act, and CGA regulations. Enhanced CDD and sanctions screening mechanisms shall be applied in high-risk jurisdictions and transactions.

5. Responsibilities

The Compliance Department and staff are responsible for monitoring all transactions to and from the company and verifying the identity of all online registered players requesting a withdrawal. They must also establish parameters by which any suspicious activity can be immediately noted, and form procedures by which to solve these issues while keeping the risk to a minimum. Such staff must follow the guidelines and requirements as per the 6th EU Anti Money Laundering Directive. The Directive requires obliged entities to verify the player in such a way that the source of funds is also identified. The verification process will be documented in such a way that every player will have a profile and if any Suspicious Transaction Report needs to be filed, all evidence in respect of the player will be in hand.

The following departments are directly targeted by the requirements of this procedure:

- **Board of Directors** – Approval and Signature requirements, especially in high risk scenarios

- **All Key Functions** – Knowledge of procedure and understanding of requirements
- **Customer Support** – Understanding reporting requirements
- **KYC Department** – Understanding and applying DD requirements
- **Sportsbook** – Understanding reporting requirements
- **Security** – Understanding DD requirements
- **Fraud** – Understanding the difference between a fraud case and an ML case
- **Finance** – Understanding the risks posed by ML/TF
- **Compliance** – Ensuring all legislation requirements are met
- **MLRO** – Updating Policy and ensuring all relevant employees are aware of AML requirements.

The MLRO/Compliance Officer shall act independently and shall not hold, nor be subordinate to, any role that may present a conflict of interest, including but not limited to the positions of CEO, CFO, COO, UBO, Casino Manager, or internal auditor.

- **Local Representative:** Luxsoft N.V. has appointed Vivian Victoria Ersilia, Managing Director of SMES Solutions for Management and Employment Support N.V., as its local representative in Curaçao to meet the CGA's requirement for a local presence. The representative can be contacted at vivian@smes.solutions.

For any questions regarding this policy, please contact: legal@gilos.io

The scope of this procedure may be extended to other departments if the need ever arises and all employees need to be attentive and aware of the information flow regarding PMLTF.

6. AML Policies and Procedures

6.1. AML Detection

Senior Management of Luxsoft N.V. are aware of the stages of money laundering and ensure to take all preventative measures to combat, prevent and detect money laundering. Prevention is ensured by carrying out the following measures:

- Implement policies and procedures throughout the group of companies;
- Clearly communicate such policies and procedures to staff;
- Adopt a risk based approach;

- Internal Controls;
- Customer due diligence procedures;
- Record keeping and Monitoring;
- Suspicious activity reporting;
- Training

6.2. Implement and clearly communicate policies and procedures to staff

Due to the size of the operation, management is principally responsible for most functions within the company. Management is aware of the policies and procedures in place throughout the group of companies. For example: withdrawals can be requested for amounts that have been turned over at least once. This protects the operator from being abused for money laundering purposes and also protects our system from free-of-charge deposits that may be abused to our disadvantage. All withdrawal requests are initially checked by the KYC department, which monitors all the withdrawal requests and denotes those which are suspicious, based on any suspected fraudulent background. Due to the size of the operation and knowledge of the player database, various customer/s due diligence and verification processes are carried out manually and automatically by KYC department. In any case where a transaction is complex or unusually large or there is an unusual pattern of transactions and the transaction has no apparent economic purpose in relation to the nature of the business, such transaction is flagged manually as suspicious, and investigations are immediately kicked off. Checks for multiple accounts, individuals which may have been blacklisted by any relevant organization or company, transaction and betting behavior, handled amounts, deposit/withdrawal methods are carried out in order to identify any suspicious activity.

6.3. Risk Based Approach

The AML Regulations imposes prevention and enforcement for subject persons. Therefore, Luxsoft N.V. applies the risk-based approach for the purposes of preventing and detecting fraud.

The following steps are followed in order to implement the risk-based approach:

- **Identification** – The identification process involves the identification of internal and

external risk factors which increase the risks being faced by the company. Predominantly, Luxsoft N.V. must assess the domestic and foreign money laundering risks affecting their target market/s. In the case scenario, whereby players are registering from countries that are non-compliant with AML Regulations and fraud management procedures, an onus is imposed on the operator to ensure that all players comply with the procedures implemented by the company. In order to actively assess and be aware of the risks the business is facing, the Business Risk Assessment (BRA) shall be reviewed at least annually and upon any significant operational or regulatory change. The updated BRA must be approved by the Board of Directors and made available to the CGA upon request. The Business Risk Assessment (BRA) addresses how gaming products/services could be exploited for ML/TF/proliferation financing.

The Company differentiates risk according to four main categories:

- a) Jurisdiction Risk
- b) Interface Risk
- c) Customer Risk
- d) Product/Service Risk

- **Assessment** – As an online gaming operator, management as well as the shareholder/s of the company understand and are aware that there is susceptibility to a certain level of high risk. Furthermore, management must stimulate awareness to detect the lack of implementation of stringent measures in order to detect fraudulent activity; the sites may become an easy target to launder money, this is a clear example of inherent risk. In carrying out the risk assessment required, the company must take into account factors relating to:

- Customers;
- the countries of geographic areas in which it operates;
- products and services including the transactions undertaken in the use of such; and
- Its delivery channels.

- **Monitoring and Follow up** –The compliance department scrutinizes the risk assessments carried out in order to recognize gaps in procedures and areas of

improvement in procedures to reduce inefficiencies. It is important to note that inefficiencies may be present in both procedures and lack of technical expertise adopted by staff.

- **Supervisory** – This process includes the review of risk assessments reviewed and the compliance department ensures that training is provided to staff involved to ensure that any updates in Regulations are applied accordingly.

6.4. Internal Controls – Implementation of the Risk Based Approach

Following the identification of inherent risk, management is required to implement the respective controls in order to mitigate such risks. The first step to adopting some form of internal control, the company must appoint at least one individual (depending on the size of the company) who is a member of the board of directors responsible for the compliance with these Regulations.

Ensure that independent testing is carried out to ensure that such controls in place are in place and do not impose any risk to the company due to present inefficiencies.

6.5. Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities and requests change as well as the services they require to be provided with.

In this respect, it is the duty of the MLRO to undertake regular reviews of the characteristics of existing Clients, new Clients, services and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented as per the Manual's requirements, as applicable, and form part of the Annual Money Laundering Report.

It is also important for the MLRO to monitor and ensure that the proper procedures are being implemented, and the risk-based approach principle is truly being followed in all areas of the Company. By doing so, one will also be ensuring that although certain products or clients may be of a higher risk, the company may continue providing these services and assisting

these clients due to the risk being mitigated through the proper policies being implemented.

6.6. Customer Acceptance Policy

The Customer Acceptance Policy (hereinafter the “CAP”), follows the principles and guidelines described in this document, defines the criteria for accepting new Clients and defines the Client categorization criteria which shall be followed by the company and especially by the employees who have direct involvement in the obtainment of information and data relating to the client as well as employees who will be tasked with evaluating such client information in order to make recommendations as to whether such client falls within the Company’s risk appetite in so far as the products or services being provided are concerned.

The Compliance department shall be responsible for applying all the provisions of the CAP. In this respect, the Compliance Officer shall also be assisting the MLRO with the implementation of the CAP, as applicable.

The MLRO shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually, in accordance with the provisions of this policy, or at any other such interval as may be determined from time to time based on any changes in the company’s inherent and residual risk.

6.6.1. Failure or refusal to submit information

Clients who fail or refuse to submit and provide the company with the requisite data, information and/or documentation for their identification and verification and the creation of their profile, after they have made their first withdrawal or due to an increase in the client risk profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Client is involved in money laundering or terrorist financing activities, although this cannot be taken as an absolute and more investigation may be required before coming to such conclusion. In such an event, the company shall suspend the customer’s account or the execution of the transaction while at the same time the MLRO must also considers whether it is justified under the circumstances at hand to submit a report to the FIU.

If, during the Business Relationship or pending the execution of a transaction, the Client fails or refuses to submit, within a reasonable timeframe (30 days from the date upon

which the relevant threshold or circumstances have become effective), the required verification data and information in accordance with this document, the company may inform the Client of their intention to terminate the Business Relationship, **provided that in so doing it will not be tipping off the client**, in which case guidance shall be sought from the FIU on how best to proceed, while at the same time examine whether it is justified under the circumstances to submit a report to FIU (STR).

6.6.2. General Principles of the CAP

The General Principles of the CAP are the following:

- (a) the company shall classify Clients and/or products into various risk categories and, on the basis of the risk perception attached to such classifications will determine the amount and quality of information and documentation which will be required in order for a client to be accepted or rejected. Such information and data must not be below the minimum requirements as set in the FIU implementing procedures and the AML Directive and PMLFTR in force at the time.
- (b) Customers may only sign up and be allowed to make use of the company's products and services if they provide the following information: (a) name and surname; (b) permanent residential address; (c) date of birth; (d) place of birth; (e) nationality; and (f) identity reference number where applicable.
- (c) all documents and data described in this policy must be collected before allowing a client to continue making use of the services provided once the thresholds have been reached (Identity Documentation and Utility Bill).
- (d) no services shall be provided to anonymous clients or clients who are known to be operating under fictitious names(s)
- (e) no services shall be provided to high-risk clients unless the prospective Client is approved by:
 - one of the Company's Director and/or Senior Managers or
 - the MLRO.

Client onboarding may be refused or terminated in cases of incomplete verification, high ML/TF risk, or sanctions exposure.

No business relationship or transaction is permitted with players listed on UN, EU, or Curaçao sanctions lists, as verified during onboarding.

All PEPs are identified through screening against public sources (e.g., Transparency International, PEP Caribbean list) and require MLRO and senior management approval prior to account activation.

6.6.3. Criteria for Accepting New Clients (based on their respective risk)

This Section describes the criteria for accepting new Clients based on their risk categorisation. Following a risk-based approach one must on a case-by-case basis determine what level of due diligence should be applied on identification, business relationship and transaction level, provided that these do not fall below the minimum as set out by the various applicable laws and regulations in place at the time. Whether the level of risk is above or below the threshold the Company is willing to undertake, one needs to be able to provide evidence to regulatory bodies that the appropriate steps have been taken to mitigate risk. There are three commonly recognised categories of due diligence.

6.6.4. Low Risk Clients

The Company shall accept Clients who are categorised as low risk Clients, as these are defined under Section 5.7 as long as the general principles as discussed in the sections below are applied.

Moreover, the Company shall follow the *Simplified Client Identification and Due Diligence Procedures* for low-risk Clients, as defined in this policy.

6.6.5. Medium Risk Clients

The Company shall accept Clients who are categorised as medium risk Clients as long as the general principles as defined in section 5.6.2 of this policy are followed.

6.6.6. High Risk Clients

The Company shall accept Clients who are categorised as high-risk Clients as long as the general principles under Section 5.10 of the Manual are followed.

Moreover, the Company shall apply the *Enhanced Client Identification and Due Diligence* measures for high risk Clients, in accordance with the measures in this policy and the due diligence and identification procedures for the specific types of high-risk Clients as

applicable.

Player Registration

In order to open an account with Luxsoft N.V. from the web portal, a user must first complete the registration process and deposit some funds with which he/she can then start playing. A risk – based approach is adopted, therefore basic principles are followed, and a checklist approach is avoided in order to remain vigilant of the customers being accepted.

The registration details to be filled in by all new customers include the first and last name, permanent residential address, country of residence, date of birth, e-mail address, phone number, gender and account currency. All customers must be at least 18 years old and can only have one player account in their name. Therefore, no minors can play on the website, furthermore, users who do not have a registered player account will not be allowed to play.

Email Verification

When a new account is created, a verification link is sent to the email account specified during the registration process. When the user clicks on the link the account is then successfully created. Only at this point can the player deposit money and start placing bets.

6.7. Customer Risk Level Breakdown

The customers will be classified as follows:

a. Low Risk (score 1 to 114)

Customers with a low-risk rating will need to undergo basic customer due diligence (as described in the Customer Due Diligence Procedure) on the first withdrawal. The customers classified as low risk will be monitored at a lower rate. Based on changes in the customer's account they can be moved to a higher risk class.

b. Medium Risk (Score 115 to 260)

Customers with a medium risk score will need to undergo basic customer due diligence (as

described in the Customer Due Diligence Procedure) on the first withdrawal. The customers classified as medium risk will be more stringently monitored (as opposed to medium-low risk customers), Level 2 account controls will be implemented. Specific Enhanced due diligence will be requested if the case arises.

c. High Risk (Score 261 to 400)

Customers with a high-risk score will need to undergo basic customer due diligence (as described in the Customer Due Diligence Procedure) on the first withdrawal. The customers classified as high risk will have the highest level of stringency applied to their ongoing monitoring. Level 3 account controls will be implemented. Full enhanced due diligence will be requested. If a customer is classified as high-risk, due diligence procedures should be initiated immediately even if no withdrawal request has been made.

d. PEPs

PEPs (Politically Exposed Persons) will be classified as their own category and will receive exceptionally stringent attention and monitoring. All customers that classify as PEPs will need to undergo compulsory due diligence as well as full enhanced due diligence including proof of wealth as well as proof of funds for all transactions higher than €500. Level 4 account controls will be implemented.

The Customer Risk Assessment is performed upon establishing a business relationship to formulate the customer's risk profile.

6.8. Customer Due Diligence

Customer due diligence can be split into 3 categories, which categories shall be dependent on the client's risk rating.

Simplified due diligence – this is the first stage of the process, which is carried out for the purposes of identifying and verifying the player. Registered details will be cross checked against any documentation and public information which includes confirmation of the name, surname, date of birth and address of the player. Such documents requested by the company may be in the form of scanned documents such as scans of the I.D. card or passport to confirm their identity. In instances where the I.D. card does not also confirm

the players' residence because no such residential information is provided on the document, then, a recent bill to confirm their address will be requested. This process may be initiated at registration or first deposit phase but does not become a requirement until the thresholds are reached. In this stage verification of source of wealth and source of funds will not require an in-depth analysis of the origin of the customer's funds and the activities which have led to the accumulation of the customer's wealth as the risk of ML/TF is relatively low. However, information in relation to said source of wealth must still be obtained, at which point a review will be undertaken of the information acquired to determine whether such information is sufficient, or further supporting documentation is required.

Customer due diligence – this is the standard process which is to be followed for the vast majority of the customer base, provided they fall within the respective risk categories requiring the application of CDD. In addition to verify the customer's identity and residential address, Luxsoft N.V. must also identify and verify the customer's source of wealth and source of funds. Luxsoft N.V. screens all players against the UN Sanctions List (<https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>), EU Sanctions List (<http://www.sanctionsmap.eu/#/main>), and any local Curaçao list of designated persons/organizations before establishing a business relationship or processing an occasional transaction. If a match is identified, the company immediately freezes the player's funds/accounts, notifies the CGA (info@cga.cw) and FIU via the goAML portal, and awaits further instructions per the Curaçao Sanctions Regime. Customer Due Diligence shall be conducted for any financial transaction equal to or exceeding NAf 4,000, whether as a single occurrence or a series of linked transactions. The company must be satisfied with sufficient certainty that the customer has provided the necessary supporting documentation which prove the origin of the customer's wealth and the activities which have led to the accumulation of the customer's wealth effectively. The customer will be allowed to deposit and making use of the company's products but will not be allowed to make any withdrawals until such time as the documentation is received. In the event that such documentation is not received within 30 days from when the company requested such information and documentation from its customers, the customer's account shall be suspended, and the customer will be precluded from depositing and making use of

the customer's products and services in addition to not allowing withdrawals to be made. A report should be sent to the MLRO within 24 hours of the happening of such an event. The MLRO shall then investigate and determine whether an STR or SAR are to be filed with the FIU.

Enhanced due diligence – this is the third and most crucial stage of the due diligence process, as further information in terms of the player is acquired. Such information includes, acquiring sound knowledge and the respective supporting documentation to confirm the proof of source of wealth of the player. This would include higher level of staff with the relevant experience as such a process requires judgement when receiving such documentation and information from the player. Upon any single or cumulative transaction, be it a withdrawal of any amount or deposit by any customer, the player will be obliged to send a proof of the source of wealth and source of funds as part of the enhanced due diligence.

No further transactions may be processed until these documents are sent by the customer and are checked and verified by the management.

This process is in line to lower the AML risks. Upon registration of a new customer, his/her transactions and betting behavior will be checked and monitored manually daily. Mechanisms are in place that enforce a one account per person policy, and if an issue of multiple accounts is detected all relative accounts are suspended/frozen until the matter is resolved. Scripts are in place that detect strange or unusual behaviors from our clients, and our software provider partners (Endorphina, Microgaming etc.) are immediately notified. This procedure enables the company to analyze the way every individual uses the products from our website, making it possible to categorize the players and thus set limits to the individual players according to their betting habits.

Customer identification and verification guidelines

In order to do a first deposit with Luxsoft N.V. a customer needs to provide the following mandatory details:

- First name
- Last name

- Gender
- Street and street number
- City and postal code
- Country
- Email address (must be valid and unique within Luxsoft N.V.)
- Date of birth
- Password (will be encrypted)
- Confirmation of password
- Account currency
- Mobile phone number

A newly registered Luxsoft N.V. account will be checked in the shortest time possible by the service department in order to find out if the details are correct (accounts with fancy names and addresses will be closed). Also, the registered country and the IP-ccountry need to be compared. A mismatch is automatically to be noted in the customers' account. This helps us close fake accounts before any pay-in can be processed.

Players who are not registered are unable and not allowed to play for real money. Any online transaction, may it be pay-in or pay-out, will not be accepted or processed.

Once the registration process has been finalised, customers will receive a welcome email with a link to access their accounts. This procedure aims at verifying the customer's email address.

Customers reaching one of the specified thresholds (first withdrawal request, suspicion of ML/TF, or increase in customer risk) go through an initial Risk assessment screening in order to determine if the customer's risk profile falls within the company's risk appetite. The following pieces of information are checked regarding each customer in order to determine the initial risk profile:

- Funding Methods
- Requested Product Type(s)
- Business Relationship Channel
- Geo-Location
- Politically Exposed Person (PEP) screening
- Sanctions Lists Screening

Each new customer has to provide a copy of an ID document (passport, ID card or driving license) when relevant thresholds are reached. This is in line with the local transposition as well as the relevant Implementing Procedures and Guidance Notes.

The identity check has to include a copy of a utility bill and/or bank statement showing the name and address and cannot consist of a mobile telephony bill.

Furthermore, the identity check may include additional measures such as the provision of a copy of each credit card used in the specific account. Further details can be found in the Procedure detailing Due Diligence process.

Any remaining doubts concerning the identity of a customer have to be reported based on the Procedure detailing reporting lines.

In such a case, further investigations have to be started.

These may include:

- Check of the IP used by the customer
- Check of the provided phone number and/or call to the provided phone number
- Internet research on the customer details
- Request to the official authorities in the country of the customer – this has to be done by compliance management.
- More information available in the dedicated CDD chapter

The due diligence criteria are set as follows:

- I.D documents must be official documents issued by a government entity that includes confirmation of the name and residential address or date of birth and a photo such as a passport can be used to verify an identity. Where this type of documentation is not available a government issued document confirming the name of the individual and supporting document supplied by a public authority, court or any financially regulated service provider that includes the individuals full name and either date of birth or residential address can be used.
- The details in the passport are compared to other documents collected at the company's discretion.

- When in doubt of forgery, the player is requested to hold up the passport to his/her face in order to verify that such passport belongs to the said individual.
- Online public databases are checked in order to cross check the information in the documents provided.
- Public searches through social media and other sources are checked in order to build the player profile.
- Finally, if it comes to our attention that the individual is a politically exposed person, enhanced due diligence is immediately carried out and the account is monitored closely.
- If the customer comes from a high-risk jurisdiction, the enhanced due diligence process is initiated immediately and the account is monitored closely. It is at the operator's discretion to refuse registrations from high-risk jurisdictions.

Sanction list Screening

The company shall on the occurrence of the following events or when it deems it fit and proper to do so, conduct a screening of the relevant sanction lists in line with its obligations and FIU implementing procedures respectively.

Upon registration, client will be screened with the various sanctions lists issued by the United Nations or the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury or the European Union or any other relevant body responsible for imposing sanctions at a worldwide level. Such screening will then be conducted periodically based on the client risk assessment conducted. The frequency of such sanction list screening will be increased should a player reach the €2,000 threshold, although such frequency will still be determined according to the client's risk. Moreover, the frequency of such screening will also be impacted by the PEP status of the particular player.

In the event that the company becomes aware that one of its clients, or potential clients, is subject to an international sanction, or has ties to countries or entities subject to such sanctions, the company must immediately inform without delay the Curaçao Gaming Authority (CGA) via their email: info@cga.cw, or in writing through the following address: The Chairman, the Curaçao Gaming Authority, Emancipatie Boulevard, Dominico F. "Don" Martina 23, Willemstad, Curaçao. All appropriate measures must be taken to ensure that any assets, including funds held on behalf of such individual, are frozen immediately until further instructions are given by the Curaçao Gaming Authority.

Prohibited Countries:

The list to be found in section A includes all countries from which the company will not be accepting any customer traffic and/or registrations.

6.9. Player Verification Procedure

Players will be requested to provide mandatory due diligence documents during the following stages:

- Upon request for the first withdrawal
- At any other stage that Luxsoft N.V.'s systems or employees detect any suspicious behavior of the Player or have any doubt on the accuracy of the information provided during the Registration Process or a Player Account classified as High Risk.

Players are obliged to provide Luxsoft N.V. with documents which verify their identity and Address. The company's employees should oversee this procedure and, where any red flags are raised or registration has been rejected and are unable to complete the registration process, the employees should manually review the documents provided and the reasons for rejection. In such cases, the employees should thoroughly check all the documents provided and third-party verification reports, and reconsider whether the documents should be accepted or rejected, and in case of rejection, whether to request the customer to provide new documents or suspend the account and report the case to the Head of Compliance/MLRO in line with the company's internal reporting procedures.

- The company's employees, in terms of player verification process, shall review the following documents:

- Documents needed to verify Players' identity:

A clear, colour, scan or photo, alongside with a selfie picture of any of the following:

- Official ID card (both sides)
- Passport (open and display the full photo ID page of the passport holder)
- Driving License (both sides)

- Documents needed to verify Players' address:

Players should provide a clear scan, colour photo, PDF or screenshot of any official document addressed to them, issued within the last 3 months, stating their full name and

current address. This can include one of the following:

- Utility bill (electricity, water, gas, landline phone bill, internet line account)
 - Bank statement or reference letter
 - Credit card statement
 - Tax/welfare letter
 - correspondence from a central or local government authority, department or agency or any other government-issued document.
- Any additional documents:

At any stage, Players may be asked to provide any further information to those already provided or any additional documentation (check Appendix B), at Luxsoft N.V.'s sole discretion.

Upon receiving the required documents and in order for the player's account to be validated, Luxsoft N.V.'s employees shall conduct a manual check on the information/documentation received and consider whether more information/documentation is needed. The following checks are to be performed:

- Check whether Player's personal data listed in the document provided matches the information provided during the registration
- Cross-Checking of any third-party report on similarity checks and whether Selfie meets the system requirements (clear photo of Player's entire face without wearing glasses, hats, scarves, or any other accessory that covers the face, in whole or in part) have been adhered to
- Make sure that system does not allow registration of Players who are underage (according to clause 5.10 - Minors Prevention Procedures), coming from restricted countries or have another Player Account in their name.
- Manual Check of documents provided to verify Players' address
- Verify the validity and authenticity documents provided
- Verify and confirm that the documents provided contain all necessary information, according to the information it is meant to verify (for a more detailed description, please check Appendix A)

6.10. Applied Due Diligence Measures and Account controls breakdown

Based on customer risk class, specific control levels will be applied to each customer

account in order to mitigate the inherent risk posed by any of these classes. The controls will be applied based on which risk criteria is more relevant when calculating customer score. The list below is by no means exhaustive and Luxsoft N.V. employees will seek guidance and advice regarding specifically suspicious accounts and situations from middle management, compliance department, MLRO and Senior management when the need for more stringent controls arises.

a. Level 1

- Proof of ID
- Proof of address
- Proof of funds (where applicable)
- Copy of Credit card (where applicable)

b. Level 2

- Controls may include but are not limited to:
- All controls mentioned for Level 1 above
- Proof of Source of Wealth
- Proof of Source of Funds

c. Level 3

Controls may include but are not limited to:

- All controls mentioned for Level 2 above
- Secondary proof of address
- Certified copies of due diligence documentation
- Video call with customer for verification purposes
- Professional/Bank Reference Letters
- Controls include but are not limited to
- Manual information review by MLRO
- Management approval for relationship continuation
- Daily account monitoring by relevant teams

Luxsoft N.V. has multiple stages of Customer Due Diligence (CDD) in place in order to mitigate as many of the risk posed by the possibility of Money Laundering and

Terrorist Financing as well as properly understand their customers as well as the nature of the intended business relationship.

To this extent specific mechanism have been put in place in order to:

- Determine who the customers are
- Verify whether that person is the person he/she purports to be
- Determine whether a person is acting on his/her own behalf or on behalf of another person
- Establish the purpose and intended nature of the business relationship, and the customer's business and risk profile
- In the case of a business relationship, monitor that relationship on an ongoing basis.

Luxsoft N.V.'s applied Due Diligence measures consist in the following:

- Identification and Verification of the Customer
- Obtaining additional information on the Purpose and Intended Nature of the Business Relationship
- Understanding and verifying the customer's source of wealth and source of funds where applicable
- Ongoing Monitoring

a. Customer Due Diligence

Luxsoft N.V., in accordance with the FIU implementing procedures requests all customers to provide standard due diligence in the following cases:

- Player requests their first withdrawal
- Any reasonable suspicion towards the player is raised
- A change in the customer's risk rating

Standard due diligence contains but is not limited to the following documents:

- Proof of Identity – This documentation will be used in order to begin verification of customer identity and will create the basis of the customer's profile. The proof of identity might consist of, but is not limited to: Copy of Local Government Issued ID, Copy of

Passport, Copy of Driver's License, Copy of Residency Card (where applicable).

- **Proof of Address** – This documentation complements the proof of identity and assures the customer has their residency where they claim they do, so proper measures can be applied to cater to their specific jurisdiction requirements. The proof of address may consist of, but is not limited to Utility Bill, Lease Agreement, Bank Statement.
- **Source of Wealth** – This piece of documentation will be used to determine the overall capacity of the player to use the funds they are using on the Luxsoft N.V. website, as well as to determine if the responsible gambling regulations are respected towards the players. Proof of source of wealth may consist of but is not limited to: Bank statement for a longer period of time, Letter from bank confirming the customer's balances, Proof of transactions that might have provided the customer with a large amount of funds.
- **Proof of funds** – This piece of documentation is required in situations where a transaction is out of the ordinary or contrary to the estimated customer rollover capacity per transaction. This is to ensure the funds used for an outstanding transaction have not been acquired by any predicate crime. Proof of funds may consist of but is not limited to: Letter from bank explaining said funds, Proof of sale (in case funds were obtained from the selling of a movable or immovable property), Bank statement specifically showing the provenience of funds used, proof of ownership of any security, proof of ownership of any legal entity and its related financial statements, dividend warrants.
- **Ongoing Monitoring** – As per regulation all customers need to undergo ongoing monitoring to a certain extent based on risk profile. A less stringent monitoring regime will be applied to customers that have scored below High Risk (for more details on risk levels please see Onboarding Procedure).

b. Enhanced Due Diligence

As per Policy all customers that pose a high risk of ML/TF, are politically exposed or it is determined that it will be more prudent to apply EDD measures, will be requested to provide extra documentation and proof of verification based on the most relevant risk factor(s). As described in the Onboarding Procedure each Risk rating warrants a different level of documentation, however if deemed necessary one or more of the following actions will be taken to ensure the customer is properly verified and the risk of ML/TF is kept under control.

The following list describes the most common documents that can be requested for Enhanced Due Diligence purposes; however, it is not exhaustive, and Luxsoft N.V. reserves the right to request any documentation to the point where management is satisfied with the customer verification:

- Copy of Debit/Credit Card – this piece of documentation is requested to verify that the deposit means used is indeed under the correct name that was collected during the initial identification and verification procedure
- Bank Statement – this piece of documentation is requested in cases where money has been transferred by means of bank transfer and helps verify that the account used for the transfer is indeed under the name collected during initial identification and verification. The Bank Statement is also used as supporting documentation for the proof of funds and wealth.
- Letter from the Bank – this piece of documentation is requested a further proof of customer's identity as well as to double check his reputability with a financial institution.
- Certified True Copies of Due Diligence Documentation – certifying the copies of the required documents offers an extra control towards the accurate verification of the customer's identity by means of a secondary licensed person checking that the documents are veritable. This can be requested when there is suspicion that the documentation might have been tampered with.
- Recorded Video Call – this action is taken when there are doubts that the person using the Luxsoft N.V. account is actually the one whose due diligence documentation has been received. Specific interactions are required on behalf of the customer to make sure that the footage is live. This procedure is not meant to eliminate the risk posed by a non-face-to-face relationship which will still be taken into consideration when analysing the customer, however it will provide extra assurance of the legitimacy of the customer's claims.
- Account Review by MLRO – this action is taken when there is suspicion of ML/TF on behalf of the customer but there is not sufficient information for filing an STR. The MLRO checks the account and gather all needed information to take a final decision regarding the ML/TF suspicion.
- Management Approval for Relationship Continuation – In cases where the customer

poses a high risk of ML/TF but does not raise any suspicion based on behaviour or documentation, express approval from management will be required to continue the business relationship.

- More Stringent Account and Transaction Monitoring – all accounts deemed as High Risk will be subject to more stringent scrutiny from the relevant teams.
- Proof of ownership of movable/immovable assets
- Proof of passive income from investments
- Proof of income from the sale of movable or immovable assets
- Proof of income from employment

c. Simplified Due Diligence

Such measures shall only be applied on low-risk scenarios, provided none of the other CDD or EDD threshold are reached. In such a case level 1 controls will be applied.

d. CDD: Player Limits and Limit Monitoring

Based on jurisdictional requirements players may need to set deposit limits upon opening an account with Company. Luxsoft N.V. staff will make sure these limits are applied. If a particular player sets their deposit limit higher than the approved amount, they will be contacted by Luxsoft N.V.'s relevant departments and will be requested to provide reasoning for their limits. Where any ML or FT suspicions come up based on the player behaviour analysis the case will be escalated to Senior Management and a EDD requirement may be triggered.

6.11. Protection of Minors and Responsible Gaming

a. Protection of Minors

Customers under the age of 18 will be denied registering an account. Customers will be required to register before playing for real money. Responsible gambling procedures will be put in place to ensure minors and persons under legal gambling age are denied access to gambling services.

The company will not accept customers unless they are of legal age (18 years or the legal age of majority in his/her jurisdiction, whichever is greater). The registration process

requires confirmation of date of birth, as well as confirmation that the customer is over 18 years of age.

Should a player still manage to go through the registration process and is under the age of 18, the Company has implemented controls in order to check and verify the age and identity of the customer. This check is carried out instantaneously upon registration by the player through Location screening. Should this check however fail for some reason, the company shall still request KYC documentation from the player upon first withdrawal. Should at any stage the player be found to be a minor, all stakes, winnings and bonuses are to be forfeited, the deposit returned (any part of it which remains) and the account blocked.

b. Responsible Gaming Measures

Luxsoft N.V. is committed to promoting responsible gaming and protecting players from gambling-related harm.

The following measures are implemented:

- **Self-Exclusion Mechanisms:** Players may opt to self-exclude from gaming for a specified period (e.g., 6 months, 1 year, or permanently) by contacting customer support. Self-excluded players are barred from accessing their accounts or creating new accounts during the exclusion period.
- **Collaboration with FMA:** The company collaborates with Fundashon pa Maneho di Adikshon (FMA) to integrate with their self-exclusion database, ensuring players who self-exclude are added to the FMA database and barred from gaming across participating operators.
- **Player Education:** The company provides resources on its website about the risks of gambling, including links to support services and information on setting deposit limits, taking breaks, and recognizing problem gambling behaviors.

6.12. Politically Exposed Persons

Luxsoft N.V. is aware of its duties towards identifying and carrying out due diligence in terms of politically exposed persons. Due to the size of the operation and awareness of our client database, currently no politically exposed persons have registered on the site.

PEPs are screened using internet searches, Transparency International Corruption Perceptions Index, www.knowyourcountry.com, and the PEP Caribbean list. Identified PEPs are subject to enhanced monitoring, EDD, and transaction approval thresholds as per Section 5.8."

The company shall apply the following with respect to the accounts of "Politically Exposed Persons":

1. The establishment of a Business Relationship or the execution of an Occasional Transaction with persons holding important public positions in Curaçao or in a foreign country and with natural persons closely related to them, may expose the Company to enhanced risks, especially if the potential Client seeking to establish a Business Relationship or the execution of an Occasional Transaction is a PEP, a member of his immediate family or a close associate of or is known to be associated with a PEP.

The Company shall pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards or who have been flagged as having regulatory deficiencies by the FATF or any other regulatory and/or monitoring authority.

2. In order to effectively manage such risks, Luxsoft N.V. shall assess the countries of origin of its Clients in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the FATF.

With regards to the issue of corruption, one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the website of Transparency International at www.transparency.org.

With regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, the Company shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.

3. PEPs are the natural persons who are residing in Curaçao or in another country and who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.

4. The meaning of a 'Politically Exposed Persons':

A PEP is a natural person who is or has been entrusted with a prominent public function, other than middle ranking or more junior officials.

The following list of some public functions in Curaçao and those held within international organisations accredited in Curaçao, which are to be considered as prominent public functions for the purpose of any regulations issued under the Prevention of Money Laundering Act: Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, Parliamentary Secretaries, and Heads of Secretariat.

5. Without prejudice to the application, on a risk-sensitive basis, of enhanced Client due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning of point

(4) above for a period of at least one year, Luxsoft N.V. shall not be obliged to consider such a person as politically exposed. Nevertheless, the Company may still consider a person to be politically exposed notwithstanding that he no longer holds an office or role which had rendered him to be considered as a PEP for a period longer than 12 months. Such decision will be based on the risk associated with the position the person had held when being considered as a PEP.

6. 'Persons known to be close associates' includes the following:

(a) any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in point (4) above

(b) any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in point (4) above.

7. Without prejudice to the provisions of this document, Luxsoft N.V. will adopt

the following additional due diligence measures when it establishes a Business Relationship or will carry out an Occasional Transaction with a PEP:

(a) Luxsoft N.V. puts in place appropriate risk management procedures to enable it to determine whether a prospective Client is a PEP. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the Client himself or from publicly available information. In the case of legal entities and arrangements, the procedures will aim at verifying whether the Beneficial Owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute PEPs. In the event of identifying one of the above as a PEP, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in this Section of the Manual

(b) the decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by an Executive Director of the Company and the decision is then forwarded to the MLRO. When establishing a Business Relationship with a Client (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the Business Relationship by an Executive Director of the Company which is then forwarded to the MLRO

(c) before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the company shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties)

(d) Luxsoft N.V. shall create the economic profile of the Client by obtaining the information specified in Section 3.2 of the FIU implementing procedures. The profile shall be regularly reviewed and updated with new data and information. The Company shall be particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks

(e) the account shall be subject to a shorter review period than would otherwise be assigned for a client of a similar risk, in order to determine whether to allow its continuance of operation. Such period shall take into account the position and measure of political

influence the PEP has as well as the inherent risk and mitigating measures associated with the products being offered to such a client. A short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the Partners and filed in the Client's personal file.

(f) Luxsoft N.V. is required to obtain a higher standard in relation to the quality of documents obtained;

Licensees may carry out or, in the case of applying enhanced on-going monitoring, implement these measures at any point in time between the establishment of the business relationship and the point in time when the Player requests their first withdrawal. In the case of an occasional transactions, licensees have to carry out the said measures, in so far as they are applicable, prior to carrying out the transaction in question.

Screening for PEP status will be carried out regularly but it is important that this is done within thirty days of the Player requests their first withdrawal, even where Luxsoft N.V. may have already screened customers to determine if they were PEPs earlier on in the course of the business relationship. Should a customer who had not been identified as a PEP at on-boarding stage result to have become one, the licensee concerned has to carry out or implement obtain senior management approval to service the PEP as well as establish what the source of wealth and, where applicable their source of funds is within the thirty day window, failing which it would have to terminate the business relationship with the said customer as described in the FIU implementing procedures.

As of 1st January 2020, the Company shall monitor the PEP registers so as to better ascertain if potential or current client is a PEP or whether any officials or related personal of a client are PEPs. Such registers are to be considered as guidance tools and one should always endeavor deeper to determine whether a person is to be considered as a PEP.

6.13. Ongoing Risk Assessment – Advanced

The player risk profile is a document describing the various items taken into consideration, when enough information is gathered regarding a player, to determine the risk said player poses to the company from an AML/CFT perspective within the confines of the Business Risk Assessment created for the company.

The player risk assessment is created in one of the following situations:

- At registration
- Player makes their first withdrawal
- Suspicion has been raised internally regarding the player's activity
- Change in Customer's PEP status
- Increase in customer risk classification
- On the detection of any red flags as defined in Annex A
- At registration an initial customer risk assessment is undertaken although such assessment will be quite limited since the player wouldn't have made any use of the company's products and no verification documentation would have been obtained at this stage.

In either of the above-mentioned cases a player risk profile is drafted and is filled in using information gathered during the business relationship. Should additional control measures be applied, the response, information and documentation provided shall also be taken into account when drafting such player risk profile.

The customer risk profile contains the following fields:

a. Username as stored in the back office

When creating an account with the company the player selects a username that will be stored within the company back office and is used to further identify the customer. The username itself cannot be utilized to identify the customer unless access is provided to the secured company back office and thus anonymization is achieved to satisfy GDPR regulation.

The only way to establish a link between the player risk profile and the player sensitive data is to have access to both platforms. Access to said platforms is carefully monitored by the company IT security team.

b. Funding method as described in the back office

The company back office stores all possible funding methods for all jurisdictions within its back office and allocates these funding methods to players using them accordingly.

Each individual payment method has received an internal relevant risk score based on the strength of the controls applied on the customers using said particular payment methods, as well as on the strength of the AML policies and procedures employed by the payment method providers themselves.

The risk scores are described as follows:

Risk Rating	Risk Score	Description
Low	4	- European or EU equivalent bank transfers - Debit cards issued by credit institutions within the EU/EEA or at EU standards
Medium	9	EU/EEA Credit Card EU/EEA PSP WHICH DO NOT ALLOW CUSTOMER TO FUND WITH CASH OR QUASI CASH
High	14	Prepaid Cards Vouchers Cash NON-EU/EEA Debit card NON-EU/EEA CREDIT CARD VFAS (crypto currencies) EU/EEA licensed payment providers that can be funded with cash or quasi- cash Non-EEA licensed PSPs that allow customers to fund with cash or quasi cash NON-EU/EEA which do not allow customer to fund with cash or quasi cash

NOTE: Some of the risk categories found in the above ratings might not be currently present within the company risk appetite, however they have been noted in the general risk assessment as to be used at any future date in case the company deems it necessary.

The current payment methods have been adjusted to reflect the current status of the company risk appetite in the individual scores.

Individual payment method scoring can be made available upon request after an NDA has been signed.

c. Player Jurisdiction

Countries banned via platform to avoid risks from an AML/CFT perspective and countries listed as High-Risk Jurisdictions subject to a Call for Action by the FATF.

The company takes into consideration player jurisdiction upon onboarding to ensure that the country the player comes from is within the company risk appetite.

All countries accepted by the platform have been analyzed based on the individual controls applied by the company on a case-to-case basis, as well as concatenating information from various online resources that offer insight on the risk specific jurisdictions pose from an AML/CFT perspective.

Each country supported by the platform has been given a risk score based on the data processed from the various resources.

The main documentation used for determining a country's risk rating are:

- The Basel Institution of Governance risk rating report
 - Transparency International Corruption Index
 - World Governance Indicator – Control of Corruption
- The jurisdiction risk scores are described as follows:

Risk Rating	Risk Score	Description
Low	8	Countries that offer a strong AML/CFT regulation in line with EU standards. Countries that offer a good AML/CFT regulation and show signs of constant improvement
Medium	17	Countries that offer an acceptable AML/CFT regulation and have shown plans to improve in the future. Countries that offer a baseline AML/CFT regulation and controls can be put in place to mitigate risks
High	25	Countries lacking sufficient and/or effective AML/CFT regulation and controls in place to mitigate risks

Blocked/Extreme	N/A	Countries banned via platform to avoid risks from an AML/CFT perspective and countries listed as High-Risk Jurisdictions subject to a Call for Action by the FATF
-----------------	-----	---

NOTE: Not all countries present in the extended score description are currently available through the platform, however scores have been assigned to the above-mentioned countries to ensure a term of comparison where needed.

A detailed list of country risk scores can be made available upon request after an NDA has been signed.

d. Game Types

The company takes into consideration the main games played by each respective player as to understand how the player's capacity to influence the game odds and knowledge of the game mechanics can influence the capacity to circulate funds through the platform.

The categorization is mainly based on the guidance offered by the Maltese FIU risk scoring and offers good insight on typology and risk rating.

All games offered by the company have been broken down into the recommended categories based on the current offer.

The top 3 games played (by number of bets initiated) will be chosen and the average will count towards to final risk score. If less than 3 games have been played in total the average will change to account for the lower number of games.

The games are categorized as follows:

RISK RATING	RISK SCORE	DESCRIPTION
LOW	6	CASINO – SLOT GAMES
MEDIUM	12	VIRTUAL SPORTS GAMES LIVE CASINO VS HOUSE
HIGH	16	P2P CASINO SPORTSBOOK E-SPORTS

NOTE: Not all games available in the general scoring table are currently available on the platform, however scoring has been added for all possible games to ensure that a risk

rating if these games are ever introduced as part of the company risk appetite.

A detailed list of games risk scores can be made available upon request after an NDA has been signed.

e. Player registration channel

The company offers the possibility of online registration for its player. On signing up players must input the details as described in section 4.8 and provide at least the first two point of level 1 controls for identification purposes. Once the player deposits and starts to wager, the account is monitored for any increase in risk or high-volume wagering/high amount wagering. Should it be deemed necessary, the client will be asked to verify the source of funds notwithstanding the fact that the relevant thresholds have not been met. Should it transpire that the information and documentation provided at this stage is fake, inaccurate or incorrect, the account will be suspended, and an investigation is initiated to determine whether there are sufficient grounds to file an STR.

The player registration channel are categorized as follows:

Risk Rating	Risk Score	Description
Low	2	Direct registration through the company's official website with email verification
Medium	5	Registration through third-party affiliates with basic verification
High	8	Registration through unverified or high-risk third-party channels

f. Player first deposit amount

The company considers that the initial sum deposited by a specific player is crucial in determining the type of behavior the company needs to exhibit towards the player from both an AML perspective as well as a Responsible Gambling perspective.

To this extent the possible first deposit amounts have been broken down to 5 categories beginning with the most common deposit amount and incrementing to the threshold for Due Diligence requirement.

The deposit amounts are broken down as follows:

Risk Rating	Risk Score	Amounts (EURO)
-------------	------------	----------------

Low	4	0 to 500
Medium	9	501 to 1000
High	11	1000 +

g. Player first withdrawal amount

The company monitors the initial withdrawal amount to determine the type of business relationship the customer seeks to form with the company as well as to place monitoring flags on the customer account for future withdrawal actions and search for any suspicious patterns.

The withdrawal amounts are broken down as follows:

Risk Rating	Risk Score	Amounts (EURO)
Low	4	0 to 500
Medium	9	501 to 1999
High	11	2000 +

6.14. Record Keeping and Monitoring

6.14.1. General

The KYC Department of the Company shall maintain records of:

- a) the Client identification documents obtained during the Client identification and due diligence procedures, as applicable; and
- b) the details of all relevant records with respect to the provision of investment services to Clients.

The documents/data mentioned above shall be kept for a period of at least five (5) years, which is to start running either from the termination of a business relationship or from the date on which an occasional transaction has been executed.

It is provided that the documents/data mentioned in points (a) and (b) above which may be relevant to ongoing investigations shall be kept by the Firm until the FIU confirms that the investigation has been completed and the case has been closed. Furthermore, should the firm require the documents for the institution, prosecution or to defend against any claim for which a longer prescriptive period exists, than such records will be kept until such time as the claim is extinguished or such prescriptive period has elapsed.

6.14.2. Format of Records

The Administration Department shall retain the documents/data mentioned in this Policy, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Administration Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to the FIU or any other relevant authority, after a relevant request.

In case the company will establish a documents/data retention policy, the MLRO shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive.

The Internal Auditor shall review the adherence of the company to the above, at least annually.

6.14.3. Certification and language of documents

1 The documents/data obtained, shall be in their original form or as a copy of the original. In high-risk cases or if deemed appropriate, the company may request documents to be certified as true copies of the original and/or be apostilled. In the case that the documents/data are certified as true copies by a different person than the company itself or by the third party with whom a reliance and or intermediary agreement has been reached, the documents/data must be apostilled or notarized or certified by a professional whose identity and professional capacity must be confirmed and verified. In certain high-risk cases, identification and verification of the certifier may also be necessary.

2 A true translation shall be attached in the case that the documents of point (1) above are in a language other than English or Maltese, or a language which is not known by the person reviewing the document.

Each time the Firm shall proceed with the acceptance of a new Client, the Head of the KYC Department shall be responsible for ensuring compliance with the provisions of points 1 and 2 above.

6.14.4. AML/CFT Audits

Luxsoft N.V. will undergo regular AML/CFT audits conducted by CGA-approved auditors to ensure compliance with the National Ordinance on Games of Chance (LOK) and other applicable regulations. Audit results will be reported to the Curaçao Gaming Authority (CGA) as required, and any identified deficiencies will be addressed promptly to maintain compliance.

6.15. On-going Monitoring Process

6.15.1. General

The regular monitoring of the Clients' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. In this respect, the MLRO shall be responsible for maintaining, as well as developing the on-going monitoring process of the Company.

6.15.2. Procedures

The procedures and frequency relating to the monitoring of Customers' profiles, accounts and examination of transactions on the basis of Client's level of risk shall include the following:

(a) the identification of:

- transactions which, as of their nature, may be associated with money laundering or terrorist financing;
- unusual or suspicious transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation;
- in case of any unusual or suspicious transactions, the administrator handling the specific client as well as the Head of that particular Department shall be responsible to communicate with the MLRO

(b) further to point (a) above, the investigation of unusual or suspicious transactions by the MLRO. The results of the investigations are recorded separately and kept in the file of the Clients concerned;

(c) the ascertainment of the source and/or origin of the funds credited to accounts;

(d) the use of appropriate IT systems;

(e) For the Company to comply with its monitoring requirements it shall review the client's

file according to the timeframes, as per section 5.15.3 below and takes into consideration the following to assess whether any additional or replacement documentation / evidence might be required:

- Update of any expired identification documentation
- Update of any changes in the companies' structure and involved persons.
- Changes in the clients' activities which might have an impact of the clients' economic profile;
- Reviewing ways in which new products and services may be used by criminals for money laundering and/or terrorist financing purposes, and how these ways may change to conceal such illicit activities;
- The compliance officer performs checks to ensure that the relevant reviews take place and documentation are kept accordingly;
- Reporting and accountability by the compliance officer to the Board of Directors and Senior Management;
- Liaising with the Curaçao Gaming Control Board, FIU, or any other relevant/appliable authority in case where such liaising is required.

6.15.3. Timeframes

The time frames set below shall act as guidelines for the KYC officer when setting the dates for the re-review dates. Such time frames may be changed if justified notwithstanding the client has been risked as in a category, provided such justification is recorded. Furthermore, these time frames shall be changed and updated should any of the factors effecting the risk the client poses will change. The below time frames shall be taken as guidance points and not as a mandatory rule.

Risk Classification Time Frames	
Low Risk	9 - 12 months
Medium Risk	6 – 8 months
High Risk	3 – 5 months

6.15.4. Payout Management Procedure

Checks to be performed on each pay-out:

a. Account check

The owner of the Luxsoft N.V. account must be the same person as the owner of the bank account, credit card or any other payment method used to send and receive funds. All account information, like address, email, date of birth etc., must be complete and authentic. Withdrawals will be made to the same source where the funds originated (where possible).

b. Deposits must have been used

On each pay-out, the company will verify whether the deposits have been used for stakes. All deposits need to have been wagered at least once (1) when a bonus was not credited before a withdrawal request can be made. In the case where a bonus has been utilised, the total amount of deposit and bonus must be wagered at least seven (7) times before being allowed to make a withdrawal. A pay-out cannot be processed if the deposited amount has not been used for stakes. If the deposited amount has not been used, the pay-out has to be denied.

Furthermore, the latest winnings have to be checked for correctness.

c. Fulfilment of bonus rules

Before a pay-out can be deducted from the customer's account, the account has to be checked if a bonus has been given to the customer since the last pay-out. When a bonus has been credited, the account has to be checked for fulfilment of the bonus rules applicable to that bonus.

If bonus rules have not been fulfilled the requested pay-out cannot be completed.

d. Deposit of funds

Funds deposited in the gaming wallet can only be used for gaming activity. Should Luxsoft N.V. notice regular changes by players to the payment method linked to the gaming wallet, the account will be temporarily suspended until the necessary explanations are provided by the player for these changes.

Luxsoft N.V. does not allow players to transfer funds between accounts under any circumstances.

Luxsoft N.V.'s KYC team continuously monitors players' deposit activity as well and has automated processes in place to receive notifications when players achieve the NAf 4,000 (four thousand) transaction limit.

e. Risk Profile for Luxsoft N.V.

The risk profile and Risk appetite for Luxsoft N.V. will be calculated based on the Business Risk Assessment done at a minimum once every year. The Business Risk Assessment will take into consideration all Risks the company faces constantly as well as the mitigating factors controlling the inherent risk. Modifications will be done to the policies and procedures for Luxsoft N.V. on the basis of the resulting residual risk, as soon as the need arises.

Withdrawals can only be paid to the same customers' account used to deposit money. In the event that the payment method used does not allow for Luxsoft N.V. to settle payouts to the same payment method, then Luxsoft N.V. must identify and verify that the method used to settle the withdrawal request belongs to the player in question.

Luxsoft N.V. does not accept cash from customers, and funds may only be received through online transfer. In the same manner no withdrawals can be processed as cash. Withdrawals will always be remitted to the same account from where the funds originated or to an account or payment method which has been verified as belonging to the player.

For every approved customer withdrawal request the company will do its utmost to process the transaction in the least possible time, in particular to not exceed 5 working days.

At all times management shall ensure that the total of all the players' account funds including any funds in transit shall be at least equal to the aggregate of the amount standing to the credit of the players' accounts held by the licensee.

CDD documentation is always requested and verified for all players effecting a single or cumulative transaction of NAf 4,000 or more (within a 180-day period) or upon requesting to withdraw funds.

The system will automatically stop minors from playing as players inputting a date of birth below the age of 18 years of age or the applicable age within their country of residence

will not be able to complete the registration process.

6.15.5. Reporting to the CGA

Luxsoft N.V. will report significant operational changes, security violations, system flaws, or fraudulent activities to the Curaçao Gaming Authority (CGA) within one day of detection. Reports will be submitted via email to info@cga.cw or in writing to the Chairman, Curaçao Gaming Control Board, Emancipatie Boulevard, Dominico F. "Don" Martina 23, Willemstad, Curaçao. Additionally, the company will submit monthly operational reports to the CGA, detailing key metrics such as transaction volumes, player activity, and compliance issues, as required under the National Ordinance on Games of Chance (LOK).

6.16. Dormant Accounts

If no transaction has been recorded on a player's account for thirty months, the account will be deemed as dormant, and the company shall do its utmost to contact the player in order to remit to him/her the remaining balance present in the account. Any funds in a dormant account are held securely. After 5 years of dormancy, unclaimed funds are transferred to a designated escrow account, and the player is notified. If the funds remain unclaimed for an additional 2 years, they are donated to a responsible gambling charity, as per Curaçao regulations.

6.17. Technical Compliance

Luxsoft N.V. complies with the technical requirements of the National Ordinance on Games of Chance (LOK) as follows:

- Audited Policies: Within six months of obtaining a license from the Curaçao Gaming Authority (CGA), the company will submit audited security policies, player account policies, and payment transaction policies to the Curaçao Gaming Authority (CGA), using CGA-approved auditors.
- RNG Certification: Within six months of licensing, the company will provide a Random Number Generator (RNG) certificate from an independent testing laboratory to the CGA.
- Server Location: The company maintains at least one physical server in Curaçao to host gaming operations, as required by the LOK.

Before launching new gaming products, payment channels, or customer interfaces, the Company shall assess potential AML/CFT vulnerabilities. Risk assessments for new technologies shall be documented and reviewed by the MLRO.

6.18. Licensing Compliance

Luxsoft N.V. holds a B2C license issued by the Curaçao Gaming Authority (CGA) under the National Ordinance on Games of Chance (LOK). The company has paid the required license fees under the National Ordinance on Games of Chance (LOK) and operates under a Green Digital Seal, indicating full compliance with CGA requirements. All operational reporting and compliance obligations, including sanctions notifications and AML/CFT audits, are managed in coordination with the Curaçao Gaming Authority (CGA) as per regulatory requirements.

7. Suspicious Activity Reporting

In any cases where the company encounters, verifies or there exists a reasonable suspicion that any form of money laundering is taking place or being attempted, such activity will be reported to the Financial Intelligence Unit of Curaçao, as required. The activity will be reported through the portal for filing and submitting of suspicious transaction reports (STR) and Suspicious Activity reports (SAR), as designated by the FIU (currently go AML portal). The company, through its MLRO is responsible to ensure that when an STR is filed, all supporting documentation and information pertaining to why the transactions, as well as the player has been flagged as suspicious must also be submitted. Any employee and/or company officer having suspicion that a client is involved in any stage of ML or TF, is attempting to launder money using the products and/or services of the company must report such suspicion to the MLRO by not later than 24 hours from when such suspicion is formed. The MLRO, upon receipt of such report, must initiate an investigation into the suspicious activity and/or transaction and verify if such suspicion is objectively justified. This is to be done in the shortest time possible. This notwithstanding, the MLRO may still continue to investigate to gather the evidence required to submit a complete SRT/SAR.

In the event that a customer is identified as a designated individual under international sanctions, the Company shall immediately freeze any associated funds or accounts, notify

the CGA and FIU, and await further instructions in accordance with the Curaçao Sanctions Regime.

The financial task force on money laundering site is checked regularly in order to keep abreast with the latest updates and blacklist jurisdictions as well as jurisdictions which do not abide to FATF and anti-money laundering regulations.

The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. Suspicion of ML/FT is subjective and one must consider a number of circumstances together in order to be able to come to a reasonable conclusion that suspicion does indeed subsist. A suspicious transaction or activity will often be one which is inconsistent with a Client's known, transaction pattern/activities or with the normal deposit/wagering activity of the specific client, or in general with the economic profile that the company has created for the Client. The company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognize on time that a transaction or a series of transactions is unusual or suspicious.

7.1. Knowledge

Knowledge may be deemed to be an objective criterion and therefore it is not difficult to ascertain whether there is ML/FT. If for any reason the MLRO, or any other employee of the Firm, is aware or is in possession of information that indicates that any of the above activities may have taken place, are taking place, or will be taking place, the MLRO should immediately proceed with filing a report with the FIU.

7.2. Suspicious Transactions

The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. Suspicion of ML/FT is subjective and one must consider a number of circumstances together in order to be able to come to a reasonable conclusion that suspicion does indeed subsist. A suspicious transaction will often be one which is inconsistent with a client's known legitimate business or personal activities or with the normal business of the specific client, or in general with the economic profile that the Firm has created for the Client. The Firm shall ensure that it maintains adequate information and knows enough about its

Clients' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

Examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing are listed in Appendix B of the Manual. The relevant list is not exhaustive nor it includes all types of transactions or services that may be requested to be used, nevertheless it can assist the Firm and its employees (especially the MLRO and the Head of the Know Your Client Department) in recognising the main methods used for Money Laundering and Terrorist Financing. The detection by the Firm of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds for the payments and intended transactions, the nature and economic/business purpose of the underlying transactions requested, and the circumstances surrounding the particular activities.

In order to identify suspicious transactions, the MLRO shall perform the following activities:

- Monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
- Monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing which is mentioned in Appendix 3 of this Manual.
- Provide any adequate training to any and all staff who will be in contact with any client, agents, client's officers, client's representatives, client's transactional information and/or documentation client's, operational information and/or documentation and any other information and/or documentation which can lead to knowledge or suspicion being detected.

Furthermore, the MLRO shall perform the following activities:

- Receive and investigate information from the Firm's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report or any other form which may be deemed appropriate from time to time in accordance with the urgency and severity of the situation. The said reports are archived by the MLRO;

- evaluate and check the information received from the employees of the Firm, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLRO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;
- if, as a result of the evaluation described above, the MLRO decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU, according to point (f) of Section 8.2 and Section 10.3 below
- if as a result of the evaluation described above, the MLRO decides not to disclose the relevant information to the FIU, then he fully explains the reasons for his decision on the Internal Evaluation Report.

7.3. MLRO's Report to the FIU

After the submission of STR/SAR reports, the company may subsequently wish to terminate its relationship with the Client concerned for de-risking reasons or to keep the account suspended until further notice/information is obtained from the FIU. In such an event, the company exercises caution, according to the Law, not to alert the Client concerned that a suspicious report has been submitted to the FIU. Close liaison with the FIU is, therefore, maintained in an effort to avoid any frustration to the investigations being conducted. If no information and/or directions are given by the FIU, it shall be up to the company to decide on the best course of action, whilst at all times ensuring that no tipping-off takes place.

Furthermore, after the submission of a suspicious transaction/activity report, the Clients' accounts and services rendered concerned as well as any other connected accounts are placed under the close monitoring of the MLRO and cease to be operative if deemed appropriate to do so without tipping off or risking tipping off the reported individual or entity.

7.4. Submission of Information to the FIU

The company shall ensure that in the case of a suspicious transaction investigation by the FIU, the MLRO will be able to provide without delay the following information:

- (a) the identity of the holders for which the services have been provided;
- (b) the identity of the Beneficial Owners;
- (c) the identity of the persons authorised to act on behalf of the Beneficial Owners;
- (d) data of the volume of funds or level of transactions used for the services being rendered and flowing through the accounts created for the Firm;
- (e) connected accounts, if any;
- (f) in relation to specific transactions:
 - the origin of the funds
 - the type and amount of the currency involved in the transaction
 - the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers
 - the identity of the person that gave the order for the transaction
 - the destination of the funds
 - the form of instructions and authorisation that have been given
 - the type and identifying number of any account involved in the transaction.
 - any other information which is available and deemed to be essential to the investigation.

In order to identify suspicious transactions, the MLRO shall perform the following activities:

- Monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
- Provide any adequate training to any and all staff who will be in contact with any client, agents, client's officers, client's representatives, client's transactional information and/or documentation client's, operational information and/or documentation and any other information and/or documentation which can lead to knowledge or suspicion being detected.

The MLRO shall belong hierarchically to the higher ranks of the Company's organisational structure so as to command the necessary authority. Furthermore, the MLRO shall lead the Company's Money Laundering Compliance procedures and processes and report to the *Senior Management*. The MLRO shall also have access to all relevant information necessary to perform his duties. The level of remuneration of the MLRO shall not

compromise his objectivity.

Furthermore, the MLRO shall perform the following activities:

- Receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report or any other form which may be deemed appropriate from time to time in accordance with the urgency and severity of the situation. The said reports are archived by the MLRO;
- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLRO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;
- if, as a result of the evaluation described above, the MLRO decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU.
- if as a result of the evaluation described above, the MLRO decides not to disclose the relevant information to the FIU, then he fully explains the reasons for his decision on the Internal Evaluation Report.
- to act as a first point of contact with the FIU, upon commencement of and during an investigation as a result of filing a report to the FIU according as indicated above;
- to ensure the preparation and maintenance of the lists of Clients categorised following a risk-based approach, which contains, among others, the names of Clients, their account number and the dates of the commencement of the Business Relationship. Moreover, the MLRO ensures the updating of the said list with all new or existing Clients, in the light of any additional information obtained;
- to detect, record, and evaluate, at least on an annual basis, or on the happening of any even which might have an impact on the overall risk, all risks arising from existing and new Clients, new financial instruments and services and update and amend the systems and procedures applied by the Firm for the effective management of the aforesaid risks should it be required and appropriate to do so;
- to evaluate the systems and procedures applied by a third party with whom the Firm

has entered into a reliance agreement in terms of Customer Due Diligence including Client Identification and Verification of the Customer, Identification & Verification of Beneficial Owners as well as the Purpose & Intended Nature of the Business Relationship applied, and approves the cooperation with such third parties;

- to ensure that all the branches and subsidiaries of the Company, if any, have taken all necessary measures for achieving full compliance with the provisions of the Manual, in relation to Client identification, due diligence and record keeping procedures;
- to provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing;
- to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing;
- to determine and whether the Company's departments and employees require further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organising appropriate training sessions/seminars. In this respect, the MLRO shall prepare and apply an annual staff-training program. Also, the MLRO assesses the adequacy of the education and training provided;
- to prepare the Annual Report, as required by the FIU and any other applicable authority;
- to respond to all requests and queries from the FIU and provide all requested information and fully cooperate with the FIU, if required;
- to maintain a registry which includes the reports of suspicious transactions, and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the MLRO, date of assessment, date of reporting to the FIU), the evaluation reports and all the documents that verify the accomplishment of his duties.
- To review the Client's files and Client Questionnaire and to approve or reject prospective High- Risk Clients.
- to develop and establish the Client Acceptance Policy and submit it to the Directors for consideration and approval;
- to review and update the Manual as may be required from time to time, and for such updates to be communicated to the Directors for their approval, at least annually or at any such period as may be deemed necessary by the MLRO;

- to monitor and assess the correct and effective implementation of the policy practices, measures, procedures and controls and in general the implementation of the Manual. In this respect, the MLRO shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Firm with the procedures and controls which are in force. In the event that the MLRO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, shall give appropriate guidance for corrective measures and where deems necessary informs the Directors and Senior Management.

8. Training

The company must ensure that training and updates are provided to staff and key persons involved in the prevention of AML and fraud within the company. Such training may be in-house or from third party providers. All training provided should be in line and in proportion to the roles and duties of the individual employee.

Training should be tailored to the tasks and duties of the employee and the company should not adopt a one size fits all approach. Training should be provided regularly and when needed. However, a yearly refresher course should be provided to ensure that all staff are up to date on recent developments.

Records of such training received must be kept on file as proof of attendance of such training.

Non-compliance with this policy may result in disciplinary actions, legal penalties under Curaçao law, and reputational damage. Violations of AML/CFT obligations may also expose the company to fine.

8.1. Employees' obligations

- (a) The Company's employees shall be personally liable for failure to report any information relating to knowledge or suspicion, regarding money laundering or terrorist financing;
- (b) the employees must cooperate and report internally, without delay, and by not later than 24 hours, anything that comes to their attention in relation to transactions for which there

are grounds for suspicion that the person is involved in money laundering or terrorist financing

(c) according to the applicable Law, the Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

8.2. Employees' Education and Training

(a) The MLRO shall ensure that the employees are fully aware of their legal obligations according to the applicable Laws, regulations, directives, and implementing procedures by introducing a complete employees' education and training program;

(b) the timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Firm. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the system of Curaçao;

(c) the training program aims at educating the Firm's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose;

(d) the training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The MLRO shall be responsible to refer to the relevant details and information in his/her Annual Report in respect of the employees' education and training program undertaken each year.

8.3. MLRO Education and Training Program

The MLRO shall be responsible for any updates in the Law and attend any external training necessary. Based on his/her training the MLRO will then provide training to the employees of the Firm further to Section 14.2 above.

The main purpose of the MLRO training is to ensure that relevant employee(s) become aware of:

- the Law and the Directive
- the Firm's Anti-Money Laundering Policy
- the statutory obligations of the Firm to report suspicious transactions
- the employees own personal obligation to refrain from activity that would result in money laundering
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

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

The MLRO shall complete a minimum of ten (10) hours of AML/CFT-specific training per calendar year, which may include workshops, webinars, or professional certifications relevant to local and international standards.

9. Agents/Intermediaries

The company shall be responsible to create and maintain its own customer base, and, for the foreseeable future, shall not engage any intermediaries or Agents nor shall it accept customers coming from such individuals or entities. Should the company decided to change its policy on the above, a more detailed policy is to be created and approved by the board of directors, highlighting the manner in which such entities will be handled in line with the applicable legislation and regulation at that time. Introducers, such as affiliates do not fall within such category as their role is to merely introduce the client to the company and will have no further involvement in the business relationship.

Annex A: List of Prohibited Countries

Australia,	Myanmar,
Austria,	Moldova,
Afghanistan,	North Korea,
Albania,	Netherlands,
Algeria,	Philippines,
Angola,	Poland,
Belarus,	Portugal,
Burundi,	Puerto Rico,
Belgium,	Pakistan,
Bulgaria,	Romania,
Central African Republic,	Saudi Arabia,
Czech Republic,	Somalia,
Colombia,	South Sudan,
Cyprus,	Sudan,
Curaçao,	Syria,
Democratic Republic of the Congo,	Serbia,
Denmark,	Sri Lanka,
Estonia,	Slovenia,

Ethiopia,	Singapore,
Ecuador,	South Korea,
Egypt,	Spain,
France and French Territories,	Sweden,
Guinea,	Switzerland,
Guyana,	Turkey,
Guinea-Bissau,	Trinidad&Tobago,
Georgia,	Tunisia,
Greece,	Yemen,
Hungary,	Ukraine (including the territory of Crimea),
Hong Kong,	United Kingdom,
Iran,	United States of America,
Iraq,	Vatican City,
Italy,	Venezuela,
Israel,	Zimbabwe
Libya,	
Latvia,	
Lithuania,	

Annex B: EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

A. MONEY LAUNDERING

Under the laws of multiple jurisdictions money laundering is a serious offence. Money laundering involves various acts committed with the intention to conceal or convert property or the proceeds derived from such property (such as money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means an offence under the Criminal Law (Penal Code) of Curaçao or any other applicable law or the equivalent law in the jurisdiction within which such offence has or is suspected to have taken place. It includes but is not limited to those offences relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion and copyright infringement amongst other.

Suspicious transactions are financial transactions that you have reasonable grounds to suspect are related to the commission of a money laundering offence. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a money laundering offence.

Suspicious transactions also include financial transactions that you have reasonable grounds to suspect are related to the commission of a terrorist activity financing offence. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a terrorist activity financing offence.

“Reasonable grounds to suspect” is determined by what is reasonable in your circumstances, including normal business practices and systems within the industry. While the Act and Regulations do not specifically require the firm to implement or use an automated system for detecting suspicious transactions, we do have such a system in place.

In this context, transactions include those that are completed or attempted as previously explained

The Company's compliance regime includes an assessment in the course of our activities, of the risk of money laundering or terrorist financing. According to this assessment, in higher risk situations, we take reasonable measures to conduct ongoing monitoring for the purpose of detecting suspicious transactions

Completed transactions

A completed transaction is one that has occurred. For example, if you process a withdrawal request from a client, a financial transaction has occurred. This is true even if the player did not wager any of the deposit, the refund of the deposit would also be a financial transaction.

Attempted transactions

An attempted transaction is one that a client intended to conduct and took some form of action to do so. An attempted transaction is different from a simple request for information, such as an enquiry as to the fee applicable to a certain transaction. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the client. A formal request by the client to withdraw funds from their account would constitute such an attempt.

The following are examples of attempted transactions:

- A financial entity or casino refuses to accept a deposit because the client refuses to provide identification as requested.
 - A securities dealer or life insurance agent refuses to process a transaction - for which the client insists on using cash - because their business practice is not to accept cash.
 - A client of a real estate agent starts to make an offer on the purchase of a house with a large deposit but will not finalize the offer once asked to provide identification.
 - An individual asks an accountant to facilitate a financial transaction involving large amounts of cash. The accountant declines to conduct the transaction.
 - A money services business will not process a request to transfer a large amount of funds because the client requesting the transfer refuses to provide identification requested.
- To report an attempted transaction, it must be one that you have reasonable grounds to suspect that it is related to money laundering or terrorist financing (as explained in section

5). An attempt to conduct a transaction does not necessarily mean the transaction is suspicious. However, the circumstances surrounding it might contribute to your having reasonable grounds for suspicion.

Transactions related to terrorist property

If an employee and/or company officer suspects that a transaction, whether completed or attempted, is related to terrorist financing, such person must raise a suspicious transaction report with the MLRO.

If such person has knowledge, rather than suspicion, that a transaction is related to funds owned or controlled by or on behalf of a terrorist or a terrorist group, then such transaction should be suspended. Accounts and/or any pending actions will be frozen or put on hold accordingly and an SAR/STR should be raised immediately.

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Client.
3. The transactions or the size of the transactions requested by the Client do not comply with his usual practice and play activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the Client's business activities or sources of income would not appear to justify such activity.
5. There is no visible justification for a Client using the services of a particular organisation. For example, the Client is situated far away from the particular organisation and in a place where he could be provided services by another organisation.
6. There are frequent transactions in the same company without obvious reason and in conditions that appear unusual (churning).
7. There are frequent purchases of services by a Client who settles in cash or transferring amounts, mainly large, with the Client's instructions, in an account other than the usual account used for the services rendered.
8. Any service requested the nature, size or frequency appear to be unusual, e.g.

cancellation of an order, particularly after the setting of the instruction.

9. The settlement of any transaction but mainly large transactions, in cash or cash equivalents.

10. Settlement of the transaction by a third person which is different than the Client which gave the order, other than in the case of an approved intermediary.

11. Instructions of transferring payment to a third person that does not seem to be related with the instructor.

12. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.

13. A Client is reluctant to provide complete information when establishing a Business Relationship about the nature and purpose of the intended business activities, anticipated accounts activities, does not disclose his source of wealth or support it adequately with documentation. The Client usually provides minimum or misleading information that is difficult or expensive for the company to verify.

14. A Client provides unusual or suspicious identification documents that cannot be readily verified.

15. A Client's home/business telephone is disconnected.

16. A Client that makes frequent or large transactions into their accounts and has no record of past or present employment or income.

17. Difficulties or delays on the submission of the financial statements or other identification documents, of a Client.

18. A Client who has been introduced by a by a third person whose countries or geographical areas of origin do not apply, or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.

19. Shared address for individuals involved in transactions with cash, or other payment methods which make it easy to disguise ownership of funds (prepaid cards, cash vouchers), particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).

20. The stated occupation of the Client is not commensurate with the level or size of the executed transactions.

21. Unexplained inconsistencies arising during the process of identifying and verifying the Client (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).

To further include in suspicious transactions:

B. TERRORIST FINANCING

When terrorist financing is pertinent, the funds may be acquired through legitimate means. Terrorist financing does not necessarily mean that the funds used were derived from criminal activities or activities of an illicit or illegal nature. The funds may be legitimate. It is not a case of disguising the source of the funds but simply the intentional transfer of funds from A to B with the intention of the receiver using those funds to support terrorist activity. The intent and the scope of such acts is different and differs from case to case, but the process used for the funding of terrorism can be fairly similar to those methods used for money laundering.

Current legislation enforces Customer Due Diligence on transactions and having this process in place has made such activity harder for those intent on transferring money for illegal activity. It is of utmost importance at Luxsoft N.V. that the policies and procedures are structured in a way that they ensure compliance with regulatory and legal frameworks, ensuring that Luxsoft N.V. is not an attractive vehicle for the purpose of terrorist financing. The company's AML policies, procedures and internal controls are designed to ensure compliance with all applicable legislations and best practice procedures. Policy is reviewed and updated on a regular basis to ensure all applicable procedures and internal controls are up to date to account for both changes in regulation and internal changes that could present new risk factors.

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating

activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding “protection” money), smuggling, thefts, robbery and drug/narcotics trafficking. Legal fund-raising methods used by terrorist groups include:

- i. collection of membership dues and/or subscriptions
- ii. sale of books and other publications
- iii. cultural and social events
- iv. donations
- v. community solicitations and fundraising appeals
- vi. Collusion on online gaming sites

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using “straw men”, false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

By: **MLRO of Luxsoft N.V.**

Name: Igor Basistii

Date: 12/11/2025



Signature

By: **UBO, of Luxsoft N.V.**

Name: Anatolii Snehirov

Date: 12/11/2025



Signature