

KLAVITORIX B.V.

V 1.1

Document

**Anti-Money Laundering/Combating
Financing of Terrorism and Financing of
Proliferation of weapon and mass
destruction (AML/CFT) Manual**

Document Information

Subject	Anti-Money Laundering and Countering Financing of Terrorism Policy
Purpose	Policy document containing policies to comply with AML Legislative and Regulatory requirements.
Involvements	All departments
Ownership	MLRO
Approval	Directors
Review	Annually or earlier as needed
Classification	Company Confidential

Change history

Date	Ver.	Author	Summary Changes	Director
21 November 2025	1.0	Anti-Financial Crime	New document created as part of AML/CFT Program review	IGA Trust B.V.
14 May 2026	1.1	Anti-Financial Crime	Updated document	

Contact information

In relation to any questions to the policy kindly contact **IGA Trust B.V.** on +5999 5145646. This policy is written to comply with the Curaçao CGA AML/CFT Guidelines for the Gaming Sector Kindly note this policy is for internal purposes only and shall not be disseminated accordingly.



MLRO

Name & Surname: Chunyan Liu
Mobile number : +356 99024202
Date: 19/05/2026



Director
IGA Trust B.V.
Date: 05/25/26

Table of contents

Document Information	1
Table of contents	2
Definitions	5
Policy Statement	6
Policy Renewal and Approval	6
Policy Ownership and Review Cycle	6
Material Triggers for Immediate Review	6
Introduction	7
Procedures	8
Key responsibilities	9
Provision of Education and Training	10
Risk Assessment	11
Business Risk Assessment	12
Business Risk Assessment Methodology	12
Products and Services Risk	13
Customer Risk	13
Delivery Channel Risk	14
Geographical Risk	14
Payment Method Risk	15
Sanctions, PEP and Adverse Media Risk	15
Terrorist Financing and Proliferation Financing Risk	15
Business Risk Assessment Summary Matrix	17
Review, Revision and Approval of the Business Risk Assessment	18
A Politically Exposed Person	19
Sanctions	20
Dealing with sanctioned persons	21
Location of Partner	21
Customer Risk Assessment	22
Managing Risks Related to Crypto Transactions	24
Approved Virtual Assets and Payment Channels	24
Prohibited Virtual Assets and Payment Channels	24
Policy and Procedures	26
Identification	26
Customer Acceptance Policy	27
Acceptance by Customer Risk Rating	27
Low-risk customers	27
Medium-risk customers	28
High-risk customers	28

Customers Not Accepted	28
PEP accounts	29
Review of screening results	29
False positive outcome	30
True positive outcome	30
Evidence of identity for participants	30
Simplified Due Diligence	32
Enhanced Due Diligence	33
Source of Funds and Wealth	33
KYC Matrix	34
Ongoing and Transaction monitoring	35
Automated Transaction Monitoring Triggers	35
Typology-Based Monitoring Triggers	36
Alert Review and Analysis Procedure	37
Outcomes of Transaction Monitoring Review	37
Ongoing monitoring	38
Escalation to MLRO	39
Refusal and Termination of the Business Relationship	39
Record keeping and retrieval of records	40
Record of Transactions	40
Retention of Records	40
MLRO and MLCO	42
Register of Money Laundering enquiries and reports	42
Internal procedures including the reporting of suspicious transactions, both internal and external	42
Internal suspicious activity reporting	43
Reporting and 'active' business	43
External suspicious activity reporting	43
Objective Indicators	44
Subjective Indicators	44
Whistleblowing Policy	45
Independent AML Audit Function	45
Staff education, training, and development	46
Importance for AML/CFT/CFR risks	46
The Importance of Staff in ML prevention	46
Human Resources Risk Factors in ML Prevention	46
Integrity	46
Staff Recruitment	46
Staff Knowledge, Training and Awareness	47

Staff promotion and transfer	48
Technological Developments	48
Proceedings	48
Offences	48
Appendices	49
Appendix A Suspicious Activity Report	49
Appendix B Banned Countries	51

Definitions

AML/CFT/CFP: Anti-Money Laundering, Combating of Terrorist Financing & Combating of Financing of Proliferation

CDD: Customer Due Diligence

EDD: Enhanced Due Diligence

FIU: Curacao Financial Intelligence Unit

FATF: Financial Action Task Force

FT: Financing of Terrorism

CGA: Curacao Gaming Authority

ML: Money Laundering

MLRO: Money Laundering Reporting Officer

NOIS: National Ordinance on identification when rendering services

NORUT: National Ordinance on the reporting of unusual transactions

OFAC: Office of Foreign Assets Control

PEP: Politically Exposed Person

SDN List: Specially Designated Nationals List

Policy Statement

Klavitorix B.V. is fully committed to maintaining compliance with all regulatory obligations set forth by the Curaçao Gaming Authority (CGA) and applicable Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and Counter Proliferation of weapons and mass destruction Financing (AML/CTF/CFP) legislation.

This policy defines the Company's approach to customer due diligence, ongoing monitoring, risk assessment, and reporting of suspicious activities. It establishes the scope, principles, and responsibilities that guide Klavitorix B.V. in ensuring robust AML/CTF/CFP controls and ethical business conduct across all operations.

The Company ensures that all directors, officers, employees, and representatives adhere to these standards and uphold the integrity of the online gaming industry by preventing the misuse of its services for money laundering, terrorist financing or proliferation of weapons and mass destruction financing purposes. Klavitorix B.V. regularly reviews and updates its AML/CTF/CFP framework to reflect evolving legal and regulatory requirements, as well as best practices.

Policy, Compliance and Review

Policy Ownership and Review Cycle

This Policy is owned by the Company's Money Laundering Reporting Officer (MLRO). In accordance with regulatory requirements, this Policy must be reviewed periodically and, at a minimum, once every 12 months. Evidence of each annual review, including any amendments made, must be recorded in the Version Control section of this Policy to provide a clear audit trail for regulators.

Material Triggers for Immediate Review

The Policy shall be reviewed earlier than the 12-month backstop if there are material changes to:

- **Legal Framework:** Applicable AML/CTF/CFP laws, regulations, or regulatory guidance.
- **Business Operations:** The Company's business model, products, services, or customer risk profile.
- **Operational Scope:** Accepted jurisdictions, payment methods, or transaction channels.
- **Risk Assessment:** Findings from the Company's Business Risk Assessment (BRA).
- **Systemic Controls:** Internal procedures, systems, controls, or third-party compliance tools.
- **Audit Outcomes:** Findings from internal reviews, external audits, regulatory inspections, or suspicious activity trends.

The company takes compliance with this policy very seriously as failing to comply puts the staff and the company at risk. We may commit a criminal offence if staff fail to comply with this policy and the AML and CTF regimes carry heavy criminal penalties according to the local jurisdictions. If any aspect of this policy, or any of the related procedures, are breached, the incident must immediately be reported to the MLRO. Due to the importance of this policy, a failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

Introduction

The aim of this manual is to set out the policies, procedures, systems and controls necessary to meet the obligations of the Company that operates from Curacao and is held to compliance with National Ordinance on identification when rendering services (NOIS) and National Ordinance on the reporting of unusual transactions (NORUT) and the Sanction National Ordinance and the Kingdom Sanction Act.

With the publication of the National Decree supervisor identification when rendering services gaming sector and the National Decree supervisor unusual transactions gaming, the Curacao Gaming Authority (GCA) is tasked with the Anti-Money Laundering, Combating of Terrorist Financing & Combating of Financing of Proliferation of weapons of mass destruction (hereinafter referred to as: AML/CFT/CFP) supervision of the gaming sector operating in and from Curaçao.

The Company acknowledges and accepts the examination, inspection and supervisory authority of the Curaçao Gaming Control Board (GCB) and the Curaçao Gaming Authority (CGA), as applicable, in relation to its licensed gaming activities and its AML/CFT/CFP obligations.

The GCB and the CGA are authorized to conduct examinations, audits, inspections and investigations, whether on-site or off-site, to assess the Company's compliance with applicable gaming, AML/CFT/CFP and related regulatory requirements. Such examinations may include, but are not limited to, reviews of policies and procedures, customer due diligence records, transaction monitoring systems, unusual transaction reporting processes, internal controls, training records and governance arrangements.

What is Money Laundering?

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is a process of making dirty money looks clean.

Please note that there are many predicate offences for money laundering such as human trafficking, arms trafficking, fraud, corruption, kidnapping and tax crimes.

What is Financing of Terrorism?

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source funds, FT is mostly concerned with obscuring the end recipient of the funds.

What is Financing of Proliferation of weapons of mass destruction?

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear chemical or biological weapons and their means of delivery and related materials.

The procedures that are appropriate for the purpose of forestalling and prevention of money laundering include:

- Identification
- Record keeping
- Staff education, training and development
- Internal procedures including the reporting of suspicious transactions, both internal and external

It is the Company's policy that NOIS and NORUT obligations to prevent money laundering are to be met in full and the company is committed to meeting and where possible exceeding such obligations.

Positive management action will be exercised to minimize the risk of the company's services and gaming activities being abused for the purposes of laundering funds associated with criminal activity, as defined by the relevant Government of Curacao legislation.

The Company will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the Curacao Financial Intelligence Unit (FIU) and thereafter shall be undertaken in conjunction with the relevant Government of Curacao authorities and in accordance with Curacao custom and practice to avoid any risk of the Company committing a tipping-off offence.

The Company's policies and procedures are based upon the regulations referred to above and associated guidance issued by the Curacao Gaming Authority.

Procedures

- All persons conducting business with the Company are properly identified, that their identity is verified where appropriate and sufficient information is gathered and recorded to permit the Company to 'know its client' and predict the expected pattern of business.
- Potential new business partners that do not appear to be legitimate are declined and where there is suspicion relating to criminal conduct on the part of a declined participant such suspicion is reported to the Money Laundering Reporting Officer (MLRO).
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation.
- All suspicions are reported promptly to Compliance
- That the Company's vigilance systems are implemented and regularly monitored.

Key responsibilities

The Company's management is responsible for:

- The day-to-day compliance with AML/CFT/CFP obligations within the areas of the Company for which they are responsible.
- Ensuring that the MLRO is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Providing the MLRO and AML/CFT/CFP Compliance Officer with the appropriate resources to fulfil their functions effectively.
- Ensuring that the MLRO has complete autonomy in the suspicious activity report evaluation process and unfettered access to information necessary to carry out that process.
- The Directors and MLRO will ensure that he/she is provided with or has access to the necessary resources to keep up to date with new money laundering requirements and developments.
- Ensuring approval of the AML/CFT/CFP program, Business Risk Assessment (BRA) and Customer Acceptance Policy (CAP).

MLRO is responsible for:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations and experience/advice from enforcement agencies.
- Representing the Company to all external agencies and any other third- party making enquiries in relation to money laundering prevention or compliance.
- Ensuring that all parts of the Company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Undertaking the internal review of all suspicions and determining whether such suspicions have substance and require disclosure to the FIU.
- All contact between the Company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.
- Establishing the suspicious reporting process and ensuring that this process is understood by all staff.
- Maintenance of the register of internal and external disclosures and register of money laundering and financing of terrorism enquiries.

AML/CFT/CFP Compliance Officer is responsible for:

- Establishing, recording, maintaining and operating appropriate procedures and controls for monitoring and testing compliance with the AML/CFT/CFP legislation.
- Adopt policies which manage the risks identified by the Company's business risk assessment, monitor the performance of these policies and address any deficiencies identified.
- Submission of a report, on at least an annual basis, to the Company's senior management that describes:
 - Any new developments within the industry in relation to AML/CFT/CFP including updates to any legislation or regulatory guidance.
 - Any updates to the Company's internal AML/CFT/CFP procedures and policies.
 - Any activities relating to compliance with the NOIS and NORUT.

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Reporting to the MLRO all knowledge or suspicions of money laundering.

- Complying fully with all money laundering procedures in respect of client identification, client monitoring, record keeping, vigilance and reporting.

Recognition of unusual transactions

This means a transaction which is inconsistent with the player profile, based on the information gathered during the course of the relationship. Based on NORIUT legislation, objective and subjective indicators have been established as a means of which the Company must assess whether a transaction qualifies as an unusual transaction. All such transactions must be reported to the compliance officer in charge, and shall be kept on file and reported to the FIU. If not reported, the reason as to why must also be documented.

Unusual transactions may qualify as the following:

- Transactions which in connection to ML/FT are reported to the police
- Transactions on behalf of a person or entity named on a list adopted by virtue of the Sanctions National Ordinance (NG 2015 no.55)
- Transactions in the amount of NAf 5000 or above regardless of the means of the payment (including cash-outs) – this may be done by way of a single transaction or a series of transactions amounting to NAf 5000, a cashless transaction in the amount of NAf 5000 or above, sale to a customer of chips in the amount of NAf 5000 or more to be done in one gaming session..

Provision of Education and Training

All members of management and staff will receive initial training and on-going training at least on an annual basis or as and when required.

Risk Based Approach

As part of the company's regulated approach to AML/CFT/CFR risk the following assessment has been conducted to adopt a risk-based approach to compliance with customer due diligence, both at the

point of registration and in relation to on-going monitoring of clients. The risk based approach encompasses both the Business Risk Assessment and the Customer Risk Assessment.

Business Risk Assessment

The Company conducts a Business Risk Assessment to identify, assess, understand, prevent and mitigate the money laundering, terrorist financing and proliferation financing risks to which the Company is exposed through its business operations.

The Business Risk Assessment forms part of this AML Policy and supports the Company's risk-based approach to customer due diligence, enhanced due diligence, customer acceptance, transaction monitoring, suspicious activity reporting, record keeping, staff training and ongoing monitoring.

The purpose of the Business Risk Assessment is to assess whether the Company's policies, procedures, systems and controls are adequate and proportionate to the risks arising from the Company's products and services, customer types, delivery channels, geographical exposure, payment methods, technologies and third-party relationships.

The Company assesses both **inherent risk** and **residual risk**.

Inherent risk means the level of ML/TF/PF risk before controls are applied.

Residual risk means the level of ML/TF/PF risk remaining after the Company's policies, procedures, systems and controls have been applied.

The Company assesses risk using the following categories:

- Low;
- Medium;
- High;

Business Risk Assessment Methodology

The Company assesses ML/TF/PF risk by considering:

- how the Company's products and services may be used to launder money, finance terrorism or finance proliferation;
- the type of customers using the Company's services;
- the jurisdictions in which customers are located, resident, registered, active or otherwise connected;
- the delivery channels through which customers access the Company's services;
- the payment methods, payment service providers and transaction channels used;
- the use of virtual assets or crypto-related payment methods, where applicable;
- exposure to sanctions, PEPs, adverse media, fraud, criminal proceeds, terrorist financing and proliferation financing indicators;
- the effectiveness of the Company's controls in preventing or mitigating those risks.

For each risk area, the Company considers:

- the nature of the risk;
- the likelihood of the risk occurring;
- the potential impact if the risk occurs;

- controls in place to mitigate the risk;
- residual risk after controls are applied;
- whether the residual risk is within the Company's risk appetite.
- The outcome of the Business Risk Assessment is used to determine the Company's Customer Risk Assessment categories, customer acceptance rules, due diligence requirements, transaction monitoring triggers, escalation procedures and risk control priorities.

The BRA is an encompassing view of inherent risks, vulnerabilities and threats to the company, the mitigating factors conducted and the residual risk, and the means and measures employed within which they are mitigated. The company's policies, internal controls, compliance management and procedural documentation, is influenced by the BRA. Every company employee is made aware of BRAs and updates, knowledge of which is tested periodically. The BRA is assessed and approved by the Board of Directors. It is made readily available to the CGA upon request.

Products and Services Risk

The Company recognises that online casino products and services may be misused for ML/TF/PF purposes, including by using the casino as a pass-through channel to deposit funds, conduct limited gameplay and withdraw funds in an attempt to create an appearance of legitimate gambling proceeds.

Product and service risks may include:

- deposit and withdrawal activity with limited or no gameplay;
- use of gambling activity to disguise the origin of funds;
- rapid movement of funds through the customer account;
- high transaction volumes inconsistent with the customer profile;
- use of bonuses, promotions or gameplay patterns to obscure fund movement;
- multiple accounts or linked accounts used to divide activity;
- customer activity inconsistent with recreational gambling behaviour.

The Company mitigates these risks through customer due diligence, customer risk assessment, transaction monitoring, gameplay monitoring, deposit and withdrawal controls, source of funds/source of wealth checks where required, escalation to the MLRO, and suspicious activity reporting where appropriate.

The Company considers the inherent risk of its products and services to be **Medium to High**, depending on customer behaviour, payment method, jurisdiction and transaction activity. The residual risk is considered acceptable only where the Company's controls operate effectively.

Customer Risk

The Company assesses the type of customers it accepts, and the ML/TF/PF risks associated with those customers.

Higher customer risk may arise from:

- customers with High Customer Risk Assessment ratings;
- customers connected to higher-risk jurisdictions;
- customers using high-risk payment methods;
- customers whose activity is inconsistent with their known or expected profile;
- customers with adverse media or public-profile concerns;
- customers whose source of funds or source of wealth is unclear;
- customers attempting to use third-party payment instruments;
- customers with unusual deposit, withdrawal or gameplay patterns;
- customers who refuse or fail to provide required information.

The Company does not accept customers whose risk falls outside its risk appetite, including:

- confirmed sanctioned persons or entities;
- confirmed PEPs, family members of PEPs or close associates of PEPs;
- customers connected to prohibited or closed jurisdictions;
- customers linked to money laundering, terrorist financing or proliferation financing;
- customers suspected of using criminal proceeds;
- customers who refuse or fail to provide required CDD, EDD, source of funds or source of wealth information;
- customers whose activity creates unresolved suspicion.

The Company mitigates customer risk through registration controls, customer due diligence, identity verification, sanctions and PEP screening, adverse media screening, Customer Risk Assessment, enhanced due diligence where required, source of funds/source of wealth checks, ongoing monitoring and offboarding where risk cannot be adequately mitigated.

Delivery Channel Risk

The Company provides its services through non-face-to-face online delivery channels. This creates increased risk because customers are onboarded, verified, monitored and serviced remotely.

Delivery channel risks may include:

- use of false or misleading customer information;
- use of VPNs, proxies or location-masking tools;
- account access from unusual or inconsistent locations;
- use of multiple accounts or linked devices;
- account takeover or use by third parties;
- difficulty confirming whether the customer is acting on their own behalf.

The Company mitigates delivery channel risk through online identity verification, duplicate account checks, device and IP indicators, account monitoring, payment method checks, sanctions and PEP screening, transaction monitoring, and escalation of unusual or inconsistent activity.

The Company recognises non-face-to-face delivery as an inherent risk factor and applies controls proportionate to the risks identified.

Geographical Risk

The Company assesses geographical risk by considering the customer's country of residence, nationality, location, payment origin, IP/device indicators where available, and other relevant jurisdictional connections.

Higher geographical risk may arise where a customer is connected to:

- sanctioned jurisdictions;
- prohibited or closed jurisdictions;
- jurisdictions subject to a FATF Call for Action;
- jurisdictions subject to FATF Increased Monitoring;
- jurisdictions with strategic AML/CFT/CFP deficiencies;
- jurisdictions associated with higher levels of corruption, organised crime, terrorism, proliferation financing, fraud or weak regulatory controls;
- jurisdictions otherwise assessed by the Company as presenting heightened risk.

The Company may reject, restrict or offboard customers connected to prohibited jurisdictions or jurisdictions outside the Company's risk appetite.

Customers connected to higher-risk jurisdictions may be subject to enhanced due diligence, source of funds/source of wealth checks, enhanced monitoring, transaction restrictions or escalation to the MLRO.

Payment Method Risk

The Company assesses the ML/TF/PF risk associated with payment methods and payment service providers.

Higher payment method risk may arise from:

- vouchers or prepaid instruments;;
- crypto or virtual asset payments;
- mobile commerce;
- multiple payment methods used by the same customer;
- payment instruments not held in the customer's own name;
- deposits and withdrawals using different payment methods;
- payment methods connected to higher-risk jurisdictions;

The Company mitigates payment method risk through approved payment channels, payment service provider due diligence, transaction monitoring, payment instrument checks where available, source of funds/source of wealth checks where required, restrictions on unsupported payment methods, and escalation of unusual activity.

Only payment methods and payment service providers approved by the Company may be used.

Sanctions, PEP and Adverse Media Risk

The Company recognises that sanctions, PEP and adverse media exposure may create increased ML/TF/PF risk.

The Company conducts sanctions, PEP and adverse media screening during onboarding and on an ongoing basis through automated tools and third-party screening services.

Confirmed sanctions matches are outside the Company's risk appetite and must not be accepted.

Confirmed PEPs, family members of PEPs and close associates of PEPs are outside the Company's risk appetite and must not be accepted.

Where a potential screening match is identified, the AML team must review the alert to determine whether it is a false positive or true positive. The review and rationale must be documented.

Where a true positive sanctions or PEP match is identified after onboarding, the account must be restricted and offboarded, subject to applicable legal, regulatory, transaction review, asset-freezing and suspicious activity reporting obligations.

Terrorist Financing and Proliferation Financing Risk

The Company assesses terrorist financing and proliferation financing risk as part of its Business Risk Assessment.

The Company recognises that TF/PF risk may arise through:

- customers connected to sanctioned persons, entities or jurisdictions;
- payment activity linked to high-risk jurisdictions;
- use of crypto assets, wallets or transaction flows connected to sanctioned exposure;
- attempts to move funds through casino activity;
- use of third-party funding or mule accounts;
- activity involving dual-use goods or proliferation-related indicators where relevant;
- unusual transaction patterns inconsistent with normal gambling activity.

The Company mitigates TF/PF risk through sanctions screening, jurisdictional controls, customer due diligence, transaction monitoring, escalation to the MLRO , and reporting where required.

Business Risk Assessment Summary Matrix

Risk area		Inherent risk	Key controls	Residual risk
Products and services		Medium / High	CDD, CRA, transaction monitoring, gameplay review, SOF/SOW checks, suspicious activity escalation	Medium
Customer types		Medium / High	Customer acceptance policy, CRA, CDD/EDD, screening, offboarding rules	Medium
Delivery channels		High	Online verification, duplicate checks, device/IP indicators, monitoring, escalation	Medium
Geography		Medium / High	Jurisdiction controls, sanctions screening, prohibited jurisdictions, EDD for higher-risk jurisdictions	Medium
Payment methods		Medium / High	Approved payment channels, PSP controls, transaction monitoring, SOF/SOW checks	Medium
Sanctions risk		High	Screening, true positive review, rejection/offboarding, reporting consideration	Low / Medium
PEP risk		High	Screening, no-PEP risk appetite, offboarding procedure	Low / Medium
TF/PF risk		High	Sanctions controls, jurisdiction monitoring, transaction monitoring, escalation and reporting	Medium

Review, Revision and Approval of the Business Risk Assessment

The Business Risk Assessment must be documented, dated and version-controlled.

The Business Risk Assessment must be reviewed whenever material changes occur to the Company's operating environment and, in any event, at least once every 12 months.

Material changes may include:

- launch of a new product or service;
 - introduction of a new technology including payment methods;
 - entry into a new jurisdiction or market;
 - change to customer onboarding or verification procedures;
 - change to transaction monitoring systems or rules;
 - change to third-party AML, KYC, payment or crypto service providers or the addition of tools and technology for AML/CFT;
 - change in applicable law, regulation or regulatory guidance;
 - sanctions or geopolitical developments;
 - findings from internal review, independent audit or regulatory inspection.
-
- Changes in typologies and trends within the remote gaming industry

The Business Risk Assessment must be reviewed by the MLRO and presented to the board.

Customer Risk Assessment

The Company conducts a Customer Risk Assessment for each customer when establishing a business relationship and updates the assessment on an ongoing basis throughout the customer relationship.

The purpose of the Customer Risk Assessment is to assess the specific money laundering, terrorist financing and proliferation financing risks to which the Company may be exposed when providing its products and services to the customer.

The Customer Risk Assessment is based on the risk categories identified in the Company's Business Risk Assessment, including customer risk, geographical risk, product and service risk, delivery channel risk, payment method risk, source of funds and source of wealth risk, sanctions risk, PEP risk, adverse media risk, and transaction risk.

Certain risk factors may not be included as weighted scoring factors because they may require mandatory escalation, manual review, enhanced due diligence, restriction, rejection or offboarding. These include sanctions exposure, PEP exposure, adverse media, unresolved source of funds/source of wealth concerns, suspected third-party activity, suspicious transaction patterns and other indicators identified in the Customer Acceptance Policy or AML procedures.

The information collected during registration, onboarding, verification, screening, payment activity, gameplay activity and ongoing monitoring is used to formulate the customer's risk profile. This includes, where available and applicable:

- date of birth and age information;

- residential address, nationality, country of residence, location, and other jurisdictional connections;
- payment methods used or intended to be used;
- actual deposits, withdrawals, gameplay activity and transaction behaviour;
- product and service usage;
- length of customer relationship and account history;

Each customer is assigned a risk rating of **Low**, **Medium** or **High**. The assigned rating determines the level of due diligence, monitoring, escalation and approval required.

The Company calculates the customer's numerical Customer Risk Assessment score using the following risk factors:

- Country Risk;
- Age Risk;
- Lifetime Risk;
- Monthly Spending Risk;
- Payment Service Provider / Payment Method Risk.

The total Customer Risk Assessment score is calculated as follows:

Total Risk Assessment Score = ((Country Risk score x 0.6) + (Age Risk score x 0.4) + (Lifetime Risk score x 0.2) + (Monthly Spending Risk score x 0.8) + (PSP Risk score x 0.8)) / 2.8

The customer is assigned a risk category based on the total score:

0 ≤ score < 20 - Low; 20 ≤ score < 50 - Medium; 50 ≤ score ≤ 100 - High

The Customer Risk Assessment must be reviewed and updated where new information becomes available or where customer activity changes materially. This includes, but is not limited to:

- the customer reaching financial transactions equal to or in excess of NAF. 4,000, or the equivalent in another currency, including linked transactions or cumulative deposits and withdrawals calculated in accordance with applicable AML/CFT procedures;
- material changes in deposit, withdrawal or gameplay activity;
- use of new or higher-risk payment methods;
- change in country of residence, nationality, location or other jurisdictional connection;
- account dormancy followed by renewed activity;

Where the customer's risk rating changes, the Company must apply the corresponding level of customer due diligence, enhanced due diligence, monitoring, escalation or offboarding measures.

Political Exposure, Sanctions and Negative Media

A Politically Exposed Person

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption. The Company does not distinguish between foreign and domestic PEPs, all are considered high risk. A PEP that no longer holds their prominent public role will also be deemed high risk.

Screening is undertaken by the Company with the help of automated tools to identify PEP and Sanctioned individuals upon customer registration/deposit. This will also pick up on any adverse media relating to the customer.

A PEP is defined as a natural person who is or has been entrusted with prominent public functions, including:

- A head of state, head of government, minister or deputy or assistant minister;
- A senior government official;
- A Member of Parliament (MP);
- A senior politician;
- An important political party official;
- A senior judicial official;
- A member of a court of auditors or the board of a central bank;
- An ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- A high-ranking officer in an armed force;
- A senior member of an administrative, management or supervisory body of a State- owned enterprise;
- A senior official of an international entity or organization.

A PEP also includes family members and close associates of the above, including:

- A spouse;
- A partner considered by national law as equivalent to a spouse;
- Other known close personal relationships such as a partner, boyfriend or girlfriend;
- A child;
- A spouse or partner of a child;
- A brother or sister (including a half-brother or half-sister);
- A spouse or partner of a brother or sister;
- A parent;
- A parent-in-law;
- A grandparent;
- A grandchild;
- A joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with a PEP;
- The sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of a PEP;
- A beneficiary of a legal arrangement of which a PEP is a beneficial owner or beneficiary;
- A person in a position to conduct substantial financial transactions on behalf of a PEP.

Klavitorix B.V. has made the decision to not accept PEPs as customers, as they fall outside the Company's risk appetite.

PEP accounts

Where a customer is flagged as a potential Politically Exposed Person, family member of a PEP, or close associate of a PEP, the following procedure applies:

Review of screening results

All PEP screening alerts generated by the Company's automated screening tools, including third-party screening services, must be reviewed by the AML team.

The AML analyst must assess the alert to determine whether it is a **false positive** or a **true positive**. This review must include, where available:

- comparison of the customer's identifying information against the screening match;
- review of name, date of birth, nationality, address, occupation, and other available identifiers;
- review of the nature of the PEP position or connection;
- review of any related adverse media, sanctions, or other risk indicators;
- documentation of the rationale for the decision.

The outcome of the review must be recorded in the customer file. The Company does not apply an automatic time limit or expiry period to PEP status.

False positive outcome

Where the AML analyst determines that the alert is a false positive, the rationale must be documented and retained.

The customer may continue to use the Company's services, subject to the Company's standard customer due diligence and ongoing monitoring procedures.

True positive outcome

Where the AML analyst determines that the customer is a true PEP match, or is a family member or close associate of a PEP, the customer must be offboarded.

From the point a true PEP match is confirmed until the account is closed, the customer will not be allowed to continue normal account activity.

The Company may restrict, suspend, or block account functionality, including deposits, withdrawals, gameplay, or other transactions, where appropriate and subject to applicable legal and regulatory requirements.

Sanctions

Sanctions are restrictions used by international communities as part of an attempt to stop financial crime and terrorism. They are designed as attempts to change the behavior of a targeted country, regime or individuals where diplomatic efforts have failed. Sanctions can take form of economic, trade, financial services, or international movement (travel bans) prohibitions.

UN Sanctions

The United Nations Security Council publishes the names of individuals and organizations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), I-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. The UN has in place other sanction lists pertaining to other jurisdictions, entities, and individuals, including wider terrorist activity under UNSR 1373.

The UN consolidated sanctions list is available at the following link:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security Policy (CFSP) objectives set out in the Treaty of the European Union. Restrictive measures imposed may incorporate UN Security Council sanctions or EU autonomous sanctions. The latter cannot be imposed against individuals or entities where there is no foreign policy dimension.

Link to the EU sanctions regimes: <https://www.sanctionsmap.eu/#/main>

The above-mentioned website also includes information about the UN sanctions regimes.

OFAC Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on the US foreign policy and national security goals against targeted foreign countries and regimes; terrorists; international narcotics traffickers; and those engaged in activities related to the proliferation of weapons of mass destruction; and other

threats to national security, foreign policy or the economy of the US. It is important to note that while US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar currency automatically engages OFAC regulations. US prosecutors take the view that if a financial transaction has cleared in the US (as do all US dollar payments, in New York), the US has jurisdiction over the offence. OFAC publishes a list of 'specially designated nationals' or SDNs (known as the SDN List) whose assets are blocked and firms, including US persons, are generally prohibited from doing business with them.

The OF AC Sanctions List Search is available at the following link:

<https://sanctionsscarch.ofac.trcas.gov/>

UK

The United Kingdom applies financial, trade, immigration, and transport sanctions through the Sanctions and Anti-Money Laundering Act 2018. These may reflect UN and EU measures or be imposed autonomously. UK sanctions are administered by the Office of Financial Sanctions Implementation (OFSI) under HM Treasury. UK persons and entities must not deal with individuals or organizations listed on the UK Consolidated List, and must report any matches.

Access the UK Sanctions List here:

<https://www.gov.uk/government/publications/the-uk-sanctions-list>

Australia

Australia enforces both United Nations Security Council sanctions and its own autonomous sanctions under the Charter of the United Nations Act 1945 and the Autonomous Sanctions Act 2011. These are administered by the Australian Sanctions Office (ASO) under the Department of Foreign Affairs and Trade (DFAT). Australian individuals and companies must ensure compliance with these measures, which include financial restrictions, travel bans, and export controls.

Information and access to the Australian Consolidated List is available here:

<https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>

Dealing with sanctioned persons

In case when the Employee during Client on-boarding, CDD or EDD procedure, or during Client ongoing monitoring becomes in the possession of the information that the Client is a sanctioned individual or has any links to sanctioned individuals and/or entities, he MUST:

- Immediately freeze all the funds / economic resources of the Client available to the Company;
- Not enter into any financial transactions or provide financial assistance or services to the Client;
- Immediately inform and file the internal report to the MLRO;
- Suspend the account of the Client until further instructions from the MLRO this is a prevention in those cases where there is a possible false positive.

It is prohibited to inform the Client or any third party (except a senior manager or MLRO) in advance, that a freezing measure is to be applied. The MLRO has to review the internal report as soon as practicable and, in case there are reasonable grounds to suspect that the Client is the sanctioned individual from the lists provided by OFAC, EU, UN or national Sanctions regimes, the MLRO will cease to conduct any further business and a report will be submitted to the FIU.

Location of Client

A customer located in a jurisdiction which is not Financial Action Task Force (“FATF”) compliant (named on FATF’s List Black or Grey), may generally be considered to represent a potential risk of money laundering or terrorist financing activity.

Therefore, customers located in jurisdictions named within the Black List will be automatically subjected to enhanced due diligence and subject to a higher degree of monitoring. However, with regards to partners resident in jurisdictions that are named within the Grey List, management considers that only with other factors, when combined with the above, create heightened risk of money laundering or terrorist financing activity. These contributory factors include but are not limited to:

- Amount of funds being transacted
- Nature and frequency of transactions
- Source of funds being transacted and the destination of the withdrawals
- Source of wealth
- The location from where the customer is accessing the platform from, if different to the registered jurisdiction (detected via IP or device checks).

A quarterly review is conducted across all registered participant jurisdictions. The review encompasses both AML/CFT/CFP and commercial considerations. The quarterly overview of the jurisdictions takes place in order to check that players have not been accepted from FATF closed or deficient jurisdictions. This review is monitored and reviewed by the senior management including the MLRO.

Managing Risks Related to Crypto Transactions

The Company recognises that virtual assets and crypto-related transactions may present increased ML/TF/PF risk due to their speed, cross-border nature, potential use of self-hosted wallets, exposure to sanctioned wallets or entities, use of mixers or obfuscation tools, and the difficulty of identifying the original source of funds in some transaction structures.

The Company applies a risk-based approach to virtual assets and crypto usage. Crypto-related services may only be offered where the related ML/TF/PF risks have been assessed, understood and mitigated through appropriate controls.

It shall be noted that the company does not offer crypto usage directly to the client but rather licenced payment providers have the option to receive funds in crypto although the company will always hold funds in FIAT

The Company does not permit unrestricted crypto activity. Crypto deposits and withdrawals may only be processed through payment methods for which are licenced financial or CASP institutions including, crypto assets, wallets, processors and transaction flows approved by the Company.

Approved Virtual Assets and Payment Channels

It shall be noted that the company does not offer crypto usage directly to the client but rather licenced payment providers have the option to receive funds in crypto although the company will always hold funds in FIAT. The payment providers used have strict controls including and ban on privacy coins or blacklisted, tainted or sanctioned wallets

A customer may not deposit or withdraw virtual assets directly to or from the Company's controlled wallet unless the transaction is processed through an approved crypto payment channel and subject to the Company's AML/CFT/CFP controls.

Prohibited Virtual Assets and Payment Channels

The Company prohibits crypto-related activity involving assets, networks, wallets, services or channels that present risks outside the Company's risk appetite or that cannot be adequately controlled. Such controls are in place and secured by the third-party CASP's on payment providers

The following are prohibited and the company ensures the third party providers ensure the following:

- anonymity-enhanced coins or privacy coins;
- shielded or privacy-enhanced transactions;
- assets or tokens on unsupported blockchain networks;
- wrapped, bridged or synthetic assets not approved by the Company;
- assets or networks not supported by the Company's approved crypto payment processor;

- manual wallet-to-wallet transfers outside approved systems;
- transfers involving customer, employee or third-party personal wallets used outside the approved payment process;
- transactions involving mixers, tumblers, chain-hopping services or obfuscation tools;
- transactions involving darknet markets, ransomware, scams, hacks, theft, fraud or other criminal exposure;
- transactions involving sanctioned wallets, sanctioned persons, sanctioned entities or sanctioned jurisdictions;
- transactions from or to prohibited or closed jurisdictions.

Where any funds are seen to be suspicious the company may refuse any transaction from a client and block any further transactions including the client's account.

The matter must be escalated to the MLRO where there is sanctions exposure, suspected ML/TF/PF, criminal exposure, unresolved suspicion, or a potential reporting obligation.

Policy and Procedures

Identification

The Company does not allow online gaming or the depositing of funds for the purpose of online gaming unless the intended participant has:

- Registered with the company through the registration page at the respective domain operated under the gaming license and
- created an account with the company and
- confirmed their acceptance of the terms and conditions.

Players must register personally and may only use an account opened in their own name. A player who has not registered themselves, or who attempts to play through an account registered by another person, will not be allowed to play.

To register, a customer must provide the company with details of their:

- First Name
- Last name
- Username (chosen)
- Date of Birth
- Email Address
- Residential Address
- Nationality

Participants registering on the site are required to input a password of their choosing. No player under the age of 18 can register with the company. If their age is below 18, they are unable to register.

Known problem gamblers will be excluded from registration as will gamblers who have previously been excluded from the site.

Records will be maintained by the Company's administration of all current, attempted and past registrations.

Upon completion of all required fields and confirmation of agreement to the terms and conditions, an email will be sent to the registered user at the email address provided. Registration will not take place if all fields are not completed. To activate the player will be required to re-log on to the respective domain using the link provided, upon successful input of their password their account will be activated.

No monies can be deposited with the company and no bonuses allocated to the account until the account has been activated.

Customer Acceptance Policy

This Customer Acceptance Policy forms part of the Company's AML/CFT/CFP framework and should be read together with the relevant provisions of this Manual, including those relating to risk assessment, business risk assessment, customer risk assessment, sanctions, PEPs and adverse media, crypto transaction risks, customer identification, simplified and enhanced due diligence, source of funds and source of wealth, the KYC Matrix, transaction monitoring, escalation to the MLRO, refusal and termination of business relationships, record keeping, and suspicious activity reporting.

The Policy is intended to:

- manage risks to which the Company may be exposed through the provision of its products and services and not exclude those client which are deemed to be 'Genuine';
- prevent the Company from being used, intentionally or unintentionally, for money laundering, terrorist financing, proliferation financing, sanctions evasion or other unlawful purposes;
- identify customers who may pose a higher than average risk; and
- ensure that customer acceptance decisions are consistent with the Company's risk appetite and applicable legal and regulatory obligations.

In applying this Policy, the Company takes into account applicable laws and regulations, regulatory guidance, sanctions requirements, the Company's Business Risk Assessment, and relevant national and supranational risk assessment materials where applicable.

Customer acceptance decisions are based on the Customer Risk Assessment, customer due diligence results, screening results, payment method risk, geographical risk, source of funds/source of wealth considerations, transaction activity, and any other relevant AML/CFT/CFP risk indicators.

The Customer Acceptance Policy determines the level of due diligence, monitoring, escalation and approval required before a customer may use the Company's products and services.

The Company will not establish or continue a business relationship where the customer falls outside the Company's risk appetite.

Acceptance by Customer Risk Rating

Following the Customer Risk Assessment, customers are classified as **Low**, **Medium** or **High** risk. Where a hard-stop indicator applies, the customer must not be accepted or must be restricted, escalated, reviewed and, where appropriate, offboarded, regardless of the customer's numerical or categorical risk rating. Should the client not be within the customer risk acceptance the relationship will be outrightly refused.

Not Acceptable Clients

The following list pre-determines the type of clients who are not acceptable or who operate within the lines of business as indicated for establishing a Business Relationship or an execution of an Occasional Transaction with the company. The following list are those customers for whom the company will not engage in a business relationship or occasional transaction. The list has been compiled throughout the operation of the company and is not exhaustive. The list hereunder shall

be updated on instances where the board of directors deem new and evolving lines of business and a high and unacceptable risk towards the company such as mentioned above shall be raised to senior management for approval of the decline and an analysis will also be made in the case where an SAR is to be raised:

- Clients who fail or refuse to submit the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification.
- Clients who have been convicted of criminal acts either by the relevant courts of Malta or in any other part of the world.
- Clients who are sanctions
- Clients who have not reached the legal age of 18+
- Clients who attempt to open account with fraudulent information, fictitious names or identity theft matters
- Clients attempting to register from Non- Reputable jurisdictions (as per internal jurisdiction scoring)
- Clients who are PEP's
- Client with intent to coming ML/FT
- Clients who are involved in business activities which are illegal, unethical or involve actions which are contrary to public order or moral standards.
- Clients who are sanctioned by international or governmental organisations.
- Individuals involved in business structures that make it impossible to verify the ultimate beneficial owner/s;
- Individuals/business structures that make it impossible to verify the legitimacy of their activities or the source of funds;
- Applicants for business who refuse to provide the required information or documentation;
- Sanctioned individuals and entities;
- Applicants for business involved in child pornography;
- Applicants for business involved in illegal drug paraphernalia;
- Applicants for business involved in pyramid sales;
- Applicants for business involved in the production or trade in radioactive materials and or arms of mass destruction;
- Applicants for business involved in the production or trade in weapons and munitions or spare parts of war related vehicles.
- Applicants for business involved in production or activities involving harmful or explosive forms;
- Applicants for business involved in forced/harmful child labour activities;
- Applicants for business involved in any form of counterfeit goods;
- Applicants who use payment processors which are registered in non-reputable jurisdictions and which are not licensed or authorised to operate in the EU.
- Individuals or entities linked to pseudo-chivalric orders or self-styled orders which are not officially recognised.
- Verification or reason to believe that funds were obtained illegally or are derived from illicit purposes.
- Client for whom an SAR/STR has been raised

- Any client who activates fraud or transactional triggers and upon analysis are found to be in a serious violation of the said account.
- Customers who refuse to explain unusual or suspicious access or who do not sufficiently explain unusual or suspicious activity on the remote gaming system.
- Customers flagged by payment providers, verification providers, law enforcement bodies or other industry collaborative platforms as potentially suspect customers or engaging in fraud, money laundering, terrorist financing etc.

Low risk Clients

- Customers registered from a country not considered to have a high risk of money laundering, terrorist financing, corruption, fraud and having completed registration with plausible identification details and complete profile information.
- verified at least the contact email or phone as applicable.
- has deposited less than €2000 in the last six months for low risk payment methods.
- customers using a limited number of payment methods which are in the customer's name.
- placed reasonable bets on the company's remote gaming products in line with "normal" gaming activity seen from regular customers with the same registration country or funding patterns.
- effect closed-loop withdrawals whereby the withdrawals are requested to the same payment method from which those funds originate and are not substantially higher than those deposited by the customer.
- customer has completed Customer Due Diligence successfully.

Medium risk customer attributes

- Customers with valid-looking registrations who register from unusual countries not targeted by the company but that are not countries with high risks of money laundering, terrorist financing, corruption, fraud, etc.
- Customers who reach the threshold of €2000 in deposits within the previous 6 months using low risk payment methods or €1,000 in deposits within the previous 6 months using low to medium payment methods.
- Customers whose betting activity is above average for a similar playing customer but not alarming.
- Customers who request withdrawals to a different payment method due to payment method inability to receive withdrawals which has been confirmed to be true.
- General customers due to the nature of the product and method of interaction.

High risk customer attributes

(if any of the attributes are identified and verified, customer will be blocked)

- Invalid or suspicious registration details, origin IP address not matching customer country, verification of email or phone not performed.
- Identity theft.
- Multiple accounts registered.
- Customer accounts used from multiple locations within an unreasonable time frame or change of pattern from normal usage.
- Customer deposits using third party payment methods or uses high risk payment methods such as quasi-cash payment methods.

- Customers that deposit unreasonable amounts in relation to their betting activity or when they would still have funds within their account which were available for betting.
- Customers who have deposited more than €2,000 over the previous year and have not yet provided a basic source of wealth information.
- Customers whose betting activity is beyond expected betting behaviour in relation to similar players and own funding sources or wealth.
- Customers who demonstrate signs of problem gambling.
- Customers who request withdrawals to alternate payment methods rather than to the origin of customer funds or request withdrawals to third party payment methods.
- Customers who refuse to provide due diligence documentation, or provide invalid or fake documentation.

Mandatory EDD clients

The instances below are those said instances where acceptance of the said customers. The company shall reserve the right, when suspicion, knowledge or reason to believe is established to further enforce enhanced due diligence, on those clients they deem necessary via an override function on the account.

- Those clients residing, registering or place of birth is within a Non-Reputable jurisdiction or the provenance of funds emanates from said jurisdiction.
- Those clients who have been risked as a high risk.
- Those clients who have been found to be associated with any negative media.
- Clients whose source of wealth and funds are deemed to be complex.

Where such a customer is identified before onboarding when it comes to a non acceptable client, the business relationship must not be established.

Where such a customer is identified after onboarding, the account must be restricted, reviewed and offboarded, subject to applicable legal, regulatory, AML/CFT/CFP, asset-freezing, transaction review and suspicious activity reporting obligations.

Evidence of identity for participants

Payments made to participants that exceed NAf 4,000 (or currency equivalent) or payments which taken cumulatively within a 30 day period exceed NAf 4,000 (or currency equivalent) are classified as qualifying payments and as such trigger the requirement for evidence to be gathered confirming the registered participant's identity.

Similarly, should a customer be deemed medium or high risk for another reason, the customer will also be subject to the following requirements.

An email will be sent automatically to the participant explaining why the payment has not yet been made and the account's activity suspended, and the following verification procedure will take place

a) Verification of identity:

The verification of identity may be completed via the verification screening conducted upon registration/first deposit depending on the information gathered. Should the screening report support enough information whereby the customer's name, address and date of birth can be relied on as being accurate then that will be sufficient for this purpose and no further information will be required from the customer. However, consideration must also be applied should there be any other suspicion, for example if you suspect that the customer is underage and is using the details of an adult to register on the platform. In such circumstances further due diligence items should be requested from the customer.

As part of the screening report, PEP, sanction and adverse media checks will also be made.

When requesting due diligence from the customer to verify their identity, the following are acceptable identity documents:

- A passport
- A national ID card
- An armed forces ID card
- A full driving license

To be acceptable identity documents must be:

- A good clear high-quality color scanned copy, plainly legible,
- Unexpired at the date of receipt,
- Bear a photo of the holder, and
- Signed by the holder

b) Verification of address:

- A recent account statement (i.e. no more than 6 months old) from a recognized bank, building society or credit card company or the most recent mortgage statement from a recognized lender.
- An unexpired photographic driving license or national identity card containing current residential address if the document has not been used to verify identity.
- A recent rates, council tax or utility bill (recent in respect of utility bills is considered to be for the last half a year i.e. no more than 6 months old). Mobile telephone bills are not acceptable as evidence of address under any circumstances.
- Correspondence from an official independent source such as a central or local government department or agency Known lawyer's confirmation of property purchase or legal document recognizing the title to the property.
- Documents provided to verify an address should not refer to P.O. Boxes or care of addresses.

For all documents, the documents should be reviewed to check the following:

- That they appear valid (e.g. the correct layout, format and style)
- That they do not appear to have been tampered with, have not expired and are within the permitted timeframes (i.e. not over 6 months for bill and account statements)
- The algorithm/MRZ on passports.

The email requesting due diligence from the customer will automatically be copied to the Administration Team. The Administration Team will log the email and await receipt of the required documents.

Should there be doubts as to the validity of a document or whether it genuinely belongs to the customer, consideration should be made as to whether the documents should be certified or that a 'selfie' photograph or video of the customer holding the document be submitted.

Open-source checks should also be conducted should there be any adverse media on the customer not detected by the verification screening checks, or to pick up on any social media that may raise further suspicions. Examples to look out for include:

- they appear to be resident in a jurisdiction different to that provided upon registration
- their lifestyle is not reflective of their level of spending on the platform
- they appear to be under the age of 18 or of a different age that to that provided upon registration
- they appear to be linked to criminal activity or terrorist organizations

The Administration Team will also consider whether a suspicious transaction report should be made to the MLRO. The factors that may influence that decision are:

- If the required documents are not received and the monies and account remain suspended after 4 weeks.
- The transaction history. If none or very few bets have been placed and a withdrawal of deposited funds is being requested, this may lead the Administration team to consider the transaction suspicious
- Multiple use of payment methods
- If bets are being placed regularly and monies won, this should not normally raise suspicions
- If a single bet is placed and large monies are won, suspicions may be raised as to the integrity of the system
- Any suspicions arise from conducting open-source checks

If suspicious activity is considered a possibility a suspicious transaction report will be lodged.

Simplified Due Diligence

Simplified Due Diligence may be applied where the Company has determined, based on its documented risk assessment, that a customer or business relationship presents a demonstrably low risk of money laundering, terrorist financing or proliferation financing. SDD is applied strictly on a risk-based basis and does not exempt the Company from customer identification, ongoing monitoring or unusual transaction reporting obligations.

SDD may be applied where all of the following conditions are met:

- The customer is assessed as low risk based on customer type, geographic exposure, product and transactional behaviour;
- The customer is not a Politically Exposed Person (PEP), nor a family member or close associate of a PEP;
- The customer is not connected to a high-risk or sanctioned jurisdiction;
-
- There are no adverse media, behavioural or transactional indicators suggesting elevated risk.

Examples of scenarios where SDD may be considered include customers demonstrating consistent recreational gaming behaviour, low transaction volumes, limited payment methods, and stable account activity consistent with the intended use of the service.

Where SDD is applied, the Company may implement proportionately simplified measures, which may include:

- Verification of identity using standard documentation without the need for additional supporting evidence;
- Reduced frequency of ongoing customer review, while maintaining continuous transaction monitoring;
- Reliance on lower thresholds for triggering further due diligence, subject to ongoing behavioural consistency.

SDD does not permit the Company to waive identification, verification, transaction monitoring or record-keeping requirements.

Enhanced Due Diligence

In certain cases, highlighted by the risk assessment, the Company may consider that a participant poses a higher risk. In these circumstances, enhanced due diligence will be requested and collected by the Company. Participants who pose an additional risk will be recorded as high risk within the administrative system and a report of their transactions and any other relevant information made available to the MLRO.

Enhanced due diligence will consist of the requirements as established for standard customer due diligence, in addition to the following:

- Requirement of additional identification data (middle names, former names, aliases, occupation, employer, personal identification number, previous addresses)
- Consideration as to whether this data needs to be further verified (additional identity documents, telephone or video call with the customer, 'selfie' with the identity document, certified documents)
- Establish the source of funds
- Establish the source of wealth
- Flag the participant for enhanced on-going monitoring
- Consideration of a further 3rd party background check
- Open source checks

A participant who poses a higher risk may be:

- Resident in a country which the company has reason to believe does not apply or insufficiently applies the FATF recommendations.
- Professional gambler
- Sporting professionals betting on sports
- Meets the EDD requirement on the risk matrix due to their level of transactions
- Meets the EDD requirement on the risk matrix due to the number of changes to their payment method.
- Any persons who are the subject of any warnings or notices.

Source of Funds and Wealth

Source of funds is quite simply the method by which the customer has deposited funds onto the platform. This should be easily identified upon the customer depositing, as the system should detect the method being used e.g. debit card or payment wallet.

Should the system not recognize the payment method, is a method unauthorized to be used on the platform, or the payment details do not match with that of the registration, all activity on the account will be suspended and the matter reported to a senior manager or MLRO.

Source of wealth is how a person has generated the money they are spending on the platform and their financial standing in general. When conducting enhanced due diligence, reasonable measures must be made to establish a source of wealth.

Source of wealth can often be satisfied by finding information in the public domain. An open-source check can offer insight into an individual's lifestyle, their occupation, the area they live and the type of home that they occupy. This information can often be found on a customer's social media account and/or looking up their address using Google Maps. Any adverse media or and media coverage in general may be picked up using verification screening systems and open-source checks respectively.

Where verification screening and open-source checks do not provide satisfactory results, documents may be requested from the customer to demonstrate their source of wealth, for example a pay slip or a contract of employment. Open-source checks can often shed light upon an individual's current employer. Each customer's source of wealth may differ entirely and therefore different approaches may need to be undertaken depending on the circumstances.

When reviewing the source of wealth information, the Company staff will need to consider how reliable or independent the source of the information is, how plausible the information is, and how this compares to the customer's activity.

KYC Matrix

Following an in-depth review of the preceding factors by the Company's senior management the following matrix details the customer due diligence requirements:

Due diligence check	Low	Medium	High
PEP, Sanction and adverse media Screening	x	x	x
Identity Verification Screening	x	x	x
Request ID and address documents		x	x
Open source checks		x	x
Source of funds	x	x	x
Source of Wealth			x
Additional identity and address			x

documents			
Additional 3rd party verification screening			x

Ongoing and Transaction monitoring

Transaction monitoring

The Company conducts ongoing transaction monitoring to identify unusual, inconsistent or suspicious customer activity, including activity that may indicate money laundering, terrorist financing, proliferation financing, structuring, pass-through activity, third-party funding, use of mule accounts, abuse of payment methods, or attempts to avoid internal or regulatory thresholds.

Transaction monitoring is conducted through automated rules, system-generated alerts, manual review by the AML team, and escalation to the MLRO where required.

The purpose of transaction monitoring is to assess whether customer activity is consistent with the customer's profile, Customer Risk Assessment, source of funds/source of wealth information, payment methods, gameplay behaviour, and expected account activity.

Automated Transaction Monitoring Triggers

The Company applies automated monitoring rules to identify customers whose activity reaches defined transaction thresholds or displays unusual transaction patterns.

The following automated threshold-based triggers are currently applied:

Trigger	Monitoring period	Description
Total deposits equal to or exceeding NAf 21,000	Last 30 days	Alert generated where the customer's total deposits reach or exceed NAf 21,000 during a rolling 30-day period.
Total deposits equal to or exceeding NAf 42,000	Last 12 months	Alert generated where the customer's total deposits reach or exceed NAf 42,000 during a rolling 12-month period.
Total deposits equal to or exceeding NAf 105,400	Lifetime	Alert generated where the customer's total lifetime deposits reach or exceed NAf 105,400

The above thresholds are monitored using aggregated customer data so that customer activity is not reviewed only on a single-project basis.

Where a threshold alert is generated, the customer's activity must be reviewed by the AML team to determine whether additional CDD, EDD, source of funds, source of wealth, enhanced monitoring, account restriction, or escalation is required.

Typology-Based Monitoring Triggers

In addition to threshold-based monitoring, the Company may apply automated or semi-automated typology-based triggers to identify suspicious transaction patterns.

The Company's transaction monitoring framework includes the following typologies.

Threat scenario	Risk description	Types of alerts
Pass-through minimal-play cash-out /	Customer uses the casino as a wash channel by depositing funds, conducting minimal gameplay, and withdrawing funds.	Withdrawal requested shortly after deposit; very low wagering ratio; net losses close to zero despite high transaction flow.
Structuring transaction splitting /	Customer attempts to avoid internal or regulatory thresholds by splitting deposits or withdrawals into smaller amounts.	Deposit amount just below threshold; high frequency of small deposits; rolling 24-hour or 30-day aggregate exceeds relevant limit.
Third-party funding / mule account	Customer funds or withdraws through payment instruments belonging to another person or linked accounts.	Payment instrument name mismatch; multiple accounts linked to the same device, IP, payment instrument or other common identifier.
Multiple payment methods and destinations	Customer obscures the source or destination of funds by rotating payment instruments or payout destinations.	High number of distinct payment instruments; high use of anonymous or higher-risk payment methods; incoming payment account differs from outgoing payment account.
Sudden change in gambling patterns	Customer shows abrupt behaviour changes that may indicate layering, account compromise or new risk.	Sudden turnover spike compared with historical activity; high betting volatility; large deposit after long inactivity.

Alert Review and Analysis Procedure

Transaction monitoring alerts do not automatically confirm suspicious activity. Each alert must be reviewed to determine whether the activity is explainable, requires further information, or gives rise to suspicion.

When reviewing an alert, the AML analyst must consider, where relevant:

- customer risk rating;
- customer identification and verification status;
- country of residence, nationality and location indicators;
- payment methods used;
- source of funds and source of wealth information, where available;
- deposit, withdrawal and gameplay history;
- wagering ratio and net loss position;
- velocity, frequency and value of transactions;
- use of multiple payment instruments;
- whether withdrawals are made to the same source as deposits;
- links to other accounts, devices, IP addresses or payment instruments;
- sanctions, PEP and adverse media screening results;
- whether the activity is consistent with the customer's known or expected profile.

The AML analyst must document the review outcome, rationale, supporting information and any action taken.

Outcomes of Transaction Monitoring Review

Following review of a transaction monitoring alert, AML Analysts may take one or more of the following actions:

- close the alert as explainable, with documented rationale;
- request additional CDD information;
- request source of funds or source of wealth information;
- apply enhanced ongoing monitoring;
- restrict deposits, withdrawals, gameplay or account functionality;
- escalate the case to the MLRO offboard the customer;
- consider whether a suspicious activity report or other regulatory report is required.

Where the customer fails or refuses to provide requested information, or where the explanation or documentation is unsatisfactory, the matter must be escalated to the MLRO.

Ongoing monitoring

Ongoing monitoring is an intrinsic part of the Due Diligence process and is mandatory for all accounts, regardless of the initial risk rating. The primary objective is to ensure that the Company remains vigilant to changes in a customer's profile and to detect unusual or suspicious activity in real-time.

The Company performs monitoring through two primary lenses:

- **Transactional Scrutiny:** The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds and that the funds are obtained from legitimate lines of business and not any business within the Customer Acceptance Policy
- **Record Keeping:** Ensuring all documents, data, and information held on the customer are accurate and kept up to date.

Any changes made to a customer's identity or personal information is processed in accordance with internal procedures. The Company will review previously provided evidence of identity and take steps to renew or update information relative to the reported changes.

- **Risk Mitigation:** While changes (such as a surname change due to marriage) are often legitimate, the Company recognizes that differing identity details may indicate an attempt to provide false information for criminal purposes.
- **Verification:** In such cases, full verification procedures will be re-applied, and the customer must provide a valid reason for the change.

The Company shall examine, as far as reasonably possible, the background and purpose of all transactions that meet any of the following conditions:

1. **Complex transactions** with no apparent economic or lawful purpose.
2. **Large transactions** that deviate from the customer's established pattern.
3. **Unusual patterns** of transactions with no visible lawful purpose.
4. **High-risk nature** transactions likely to be related to ML/FT.

Ongoing monitoring serves as a trigger for dynamic risk assessment. Transactional alerts will lead to immediate scrutiny to establish if suspicious activity is occurring.

- **System Documentation:** A full review of both identity verification and transaction history will be conducted. A mandatory note must be left in the system detailing the checks performed and the final result.
- **Risk Overrides:** Management may manually override and increase a risk rating at any time. A higher risk rating dictates a more frequent review cycle and stricter monitoring parameters.

A manual review of the account can be conducted at the situations which present a risk of ML/FT to ensure the client is properly assessed. Open source intelligence is also to be used and to corroborate SOW/F information provided, this shall be carried out on those clients for which have raised concern in relation to the funding of the account or upon review. If there is a mismatch between the information provided by the Client and background research, this could lead to a ML/FT concern leading to the Client being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

While monitoring is continuous, formal periodic reviews of the Customer Risk Assessment (CRA) are required as a backstop. These reviews are conducted from the date of the last assessment based on the risk level:

- High Risk: 12 months
- Medium Risk: 24 months
- Low risk : 30 months

Escalation to MLRO

The AML team must escalate a transaction monitoring case to the MLRO where:

- activity may indicate ML/TF/PF;
- structuring or threshold avoidance is suspected;
- third-party funding or mule account activity is suspected;
- funds may be linked to criminal proceeds;
- sanctions exposure is identified;
- the customer refuses or fails to provide required information;
- source of funds or source of wealth cannot be reasonably established;
- the customer's activity remains unusual or unexplained after review;
- the case may require suspicious activity reporting.

The MLRO is responsible for determining whether a suspicious activity report or other regulatory report is required.

Refusal and Termination of the Business Relationship

In accordance with Article III.8 of the Curaçao AML Regulation, the Company shall refuse to establish or shall terminate an existing business relationship where it is unable to comply with applicable customer due diligence requirements.

This includes, but is not limited to, circumstances where:

- The Company is unable to identify and verify the customer's identity or, where applicable, the beneficial owner;
- The Company is unable to obtain sufficient information on the purpose and intended nature of the business relationship;
- Required enhanced due diligence measures cannot be completed for high-risk customers;
- The customer fails or refuses to provide requested information or documentation without reasonable justification;
- There are reasonable grounds to suspect that the relationship or transactions are connected to money laundering, terrorist financing or proliferation financing, and the risks cannot be adequately mitigated;

Cases meeting the above criteria are escalated to the MLRO or a designated senior Compliance officer for assessment. The decision to refuse or terminate a business relationship is taken by the MLRO.

All decisions, supporting rationale and actions taken are fully documented and retained in accordance with record-keeping requirements.

Record keeping and retrieval of records

Record of Transactions

The Company will maintain appropriate records of all participants and their associated transactions. The MLRO has unfettered access to all records (other than those which are stored in an encrypted or hashed form) and reporting through the back-office computer system.

- Identification and verification of identity

The MLRO will at all times retain access to the back-office computer system which holds the registration details of all participants. Such records can be accessed without delay via bespoke reports accessed/generated by the back-office system.

The MLRO has the ability to retrieve all identity verification that has been collated on all customers. This includes all correspondence between the Company and the customer, plus any notes and internal investigations conducted on customer activity.

- Deposits, withdrawals, bets, prize payments, credits

All financial transactions are recorded against the customer within the back-office system and are reconciled against source of funds data. This includes the name of the participant or unique identity number, the amount and nature of the transaction, the date of the transaction, the source or recipient of the funds and the nature of the financial transaction (credit/debit card, e-wallet etc.)

All financial transactions are maintained in a system audit log which is available to the MLRO at all times.

Each transaction is recorded in the database of the website with a specific reference. Transactions are sorted in the back-office using the same reference pattern and can be scrutinized by the MLRO by date, participant or nature of the transaction.

- Internal compliance documents – policies and procedures, internal and external registers and reports, risk assessments, staff vetting and training, reports prepared by the AML/CFT/CFP Compliance Officer for the management.

All internal compliance documents will be held on the back-office system, with the MLRO having full access.

Retention of Records

All the above-named records will be maintained in a secure and accessible form. Secure backups are made daily of the following customer data:

- Records
 - all registration details
 - identification verification details
 - standard and enhanced due diligence items
 - suspended accounts and reason for suspension
 - closed accounts
 - financial transactions – deposits, bets made, withdrawals, prize payments
 - self-exclusion periods (temporary and permanent)

- self-imposed limits
- excluded players
- complaints and responses
- audit trails
- bank reconciliations
- Customer Service electronic correspondence records

Records associated with a customer (including all identification records and the financial transactions made by them) are maintained for a period of 5 years after the date of closure of the customer's account or the date of the last transaction.

Records associated with the register of internal and external disclosures and the register of money laundering and financing of terrorism enquiries will be maintained for a period of 5 years following the finalization of the relationship with the related parties or for the period as advised by the FIU.

MLRO and MLCO

Register of Money Laundering enquiries and reports

The MLRO maintains a register separately from other records associated with the company which details:

- a) Enquiries made to the Company by law enforcement or other officials acting under powers provided by the Money Laundering and Terrorist Financing Requirements

This register contains:

- The nature and date of the enquiry
- The name of the enquiring officer and enforcement agency
- The powers being exercised
- Details of the participant
- Details of the transaction
- Outcome of enquiry (if known)

- b) All reports made to a representative within the FIU in relation to suspicious transactions.

This register contains:

- The name of whom the report is made (MLRO)
- Relevant dates of the suspicious activity and when internal and external
- Information about the activity which is sufficient to identify the grounds for suspicion
- The reference number supplied by the FIU
- Outcome of enquiry (if known)
- Any other disclosure made to the FIU for intelligence purposes only

- c) All reports made to the MLRO by the Company employees.

This register contains:

- The nature and date of the report including details of the participant and the transaction
- The name of the person making the report
- Information about the transaction which is sufficient to identify the relevant papers
- Details of the acknowledgement of receipt of report provided by the MLRO or DMLRO
- Whether or not it was escalated to be reported to the FIU
- Outcome of the report

Internal procedures including the reporting of suspicious transactions, both internal and external

The Company shall at all times have an appointed MLRO. The appointed MLRO will be sufficiently senior within the company and will have the right of direct access to the Directors of the Company.

The MLRO will have unfettered access to all reports, transaction histories, complaints and audit trails.

The Company applies specific logic to identify linked transactions that, when considered collectively, may constitute an unusual transaction even if individual transactions appear normal in isolation. Linked transaction detection includes:

- Aggregation logic, whereby multiple transactions conducted by the same customer within a defined period (e.g. daily, weekly or monthly) are assessed cumulatively against regulatory thresholds;
- Behavioural linkage, including repeated transaction patterns that demonstrate consistent structuring, such as multiple deposits or withdrawals just below reporting thresholds;
- Account linkage, including analysis of shared identifiers such as IP addresses, devices, payment instruments, registration details or behavioural markers to detect coordinated activity across multiple accounts.

Where linked transactions are identified, they are assessed as a single transactional event for the purposes of determining whether an unusual transaction has occurred.

Internal suspicious activity reporting

Suspicious must be reported to the MLRO as soon as reasonably practical using the attached form, as per Appendix A. The form is also available on request from the MLRO. The case may be discussed initially with the MLRO, but a telephone discussion is not a substitute for formal notification using the appropriate form.

It is important that the form is used as this properly documents the report itself and ensures that all relevant information is included. For this reason, it is important that all parts of the form are completed.

Receipt of the report will be acknowledged by the MLRO. It is necessary for the person making the report to include their name on it. Once an initial report has been submitted the person should continue to submit reports where further suspicious activity takes place, or if there are developments in respect of the matter originally reported.

Reporting and 'active' business

Where a suspicion is reported in respect of a transaction that has not taken place or an activity that has not commenced this fact should be made clear to the MLRO. If the person submitting the report is involved with the transaction or activity, they should not do anything further until advised that they can do so by the MLRO.

The MLRO in conjunction with the Directors will manage the process of ensuring that the transaction may proceed, including obtaining FIU clearance if appropriate.

External suspicious activity reporting

The MLRO has full access to information and records of the company that the Directors consider necessary to evaluate internal reports received. They will document the evaluation process and the reasons for conclusions reached.

If after completing the evaluation process the MLRO considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the MLRO is responsible for:

- Submitting the necessary information to the FIU.
- Recording the disclosure in the register of disclosures.
- Dealing with subsequent production or account monitoring orders if there are any.

Tipping Off/Confidentiality

Any person must treat any information where that person knows or suspects that an unusual transaction report has been made or that an investigation is under way or proposed or strictly confidential.

No staff member may disclose to any person s/he has formed a suspicion that a person may be involved in suspicion that a person may be involved in suspicious matters or transactions or that a report has been lodged about that person with the FIU or any other authority.

Clear lines of reporting where matters or transactions are referred to the MLRO need to be maintained. All matters or transactions are to remain confidential between the reporting staff member and the MLRO.

It is an offense to disclose that an unusual transaction report or related information on a specific transaction has been reported to the FIU or that an investigation into money laundering, terrorist financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

Objective Indicators

1. Transactions reported to law enforcement

Any transaction that is already reported to the police or judicial authorities in connection with money laundering, terrorist financing or other predicate offences.

2. Sanction-listed Parties

Any proposed transaction by or for the benefit of a natural or legal person, group or entity whose name appears on a sanctions list compiled under the relevant National Sanctions Ordinance.

3. High-Value Transactions

Any transaction involving an amount equal to or exceeding the equivalent of 5,000 NAF, regardless of payment method.

This includes the following sub-categories:

- Giro-based transfers initiated at the client's request (bank/wire transfers)
- Deposits or withdrawals of funds at client request
- Sale of gaming tokens (chips, credits) to a client
- Payout of winnings or prize funds
- Any other transaction that meets the amount threshold

Subjective Indicators

Transactions giving reason for suspicion

Any transaction that gives cause to assume that it may be connected with money laundering or terrorist financing based on the facts and circumstances of the transaction, even if objective criteria are not met.

Whistleblowing Policy

If, in the course of employment, an employee becomes aware of information which they reasonably believe tends to show one or more of the following, they must use the Company disclosure procedure set out in the Whistleblowing Policy:

- That a criminal offence has been committed is being committed or is likely to be committed.
- That a person has failed, is failing or is likely to fail to comply with any legal obligation to which they are subject.
- That a miscarriage of justice that has occurred, is occurring, or is likely to occur.
- That the health or safety of any individual has been, is being, or is likely to be endangered.
- That the environment has been, is being, or is likely to be damaged.
- That information tending to show any of the above, is being, or is likely to be deliberately concealed.
- That the business or any associated person has been, is being, or is likely to be receiving or offering bribes.
- That any foreign official has been, is being, or is likely to be bribed or offered facilitation payment by the Company or any associated person.

Independent AML Audit Function

The Company ought to maintain an independent audit function to assess the effectiveness, adequacy and compliance of its AML/CFT/CFP framework. The purpose of the independent audit is to provide objective assurance that the Company's policies, procedures, systems and controls are designed and operating effectively in accordance with applicable laws, regulations and supervisory guidance.

The independent audit covers, at a minimum, the following areas:

- Governance and oversight of the AML/CFT/CFP framework, including the role and effectiveness of the MLRO;
- Customer due diligence, enhanced due diligence and ongoing monitoring processes;
- Transaction monitoring, unusual transaction detection and UTR reporting procedures;
- Sanctions screening and PEP identification controls;
- Risk assessment methodologies, including customer, product, geographic and delivery channel risks;
- Record-keeping and data retention practices;
- AML training and awareness programs;
- Compliance with regulatory reporting and internal escalation requirements.

The scope may be expanded based on the Company's risk profile, regulatory developments or findings from previous audits.

- The independent audit function operates independently from the Company's operational and compliance functions. Individuals or entities performing the audit:
- Are not involved in the design, implementation or day-to-day operation of the AML/CFT/CFP framework;
- Do not report to the MLRO or Compliance function in relation to audit activities;
- Have no conflicts of interest that could impair their objectivity or impartiality.

The audit may be conducted by an internal audit function with appropriate independence or by an external third-party audit firm with demonstrated AML/CFT expertise.

The results of the independent audit are reported to senior management and, where applicable, the Board or equivalent governing body. Material deficiencies are escalated without undue delay and are tracked until fully remediated.

Staff education, training, and development

Importance for AML/CFT/CFR risks

The way the company is organized can increase or mitigate the exposure of the company to money laundering and terrorist financing risks. Procedures and controls operated by the company, many of which are required by law, can be applied in order to manage AML/CFT/CFR risk.

The Importance of Staff in ML prevention

Success in preventing money laundering and terrorist financing cannot be achieved by having appropriate policies alone. Even the best policies are useless if staff ignore or circumvent them, whether through ignorance, carelessness or deliberately. Staff are a business's strongest defense or their weakest link.

Human Resources Risk Factors in ML Prevention

The main human resources risk factors are:

- Staff lack integrity.
- Staff lack knowledge, training or awareness.
- Staff have conflicts of interest.
- Direct criminal or terrorist exploitation of HR weaknesses.

Integrity

The integrity of the directors and employees of the Company are the foundation of its AML/CFT/CFR measures. If staff lack integrity there is a danger that they may become involved in or become willing accomplices to laundering activity.

Direct involvement in laundering operations is the possible extreme. More likely is that staff without the right attitude are unlikely to:

- Maintain awareness and detect money laundering.
- Report money laundering if they become aware of it.
- Take seriously their own training or that of their subordinates.
- Encourage reporting and foster a culture that supports money laundering prevention.

Staff Recruitment

It is important that we take appropriate steps to ensure the integrity of new staff. Such steps should be risk based, with the extent of the effort proportional to the role of the employee and the money laundering threat inherent in the role they are being recruited for.

The following staff screening procedures are operated by the Company:

- For all new staff at least one reference will be taken up. References will be obtained by obtaining the permission of the prospective employee to write direct to the referee. References supplied by the prospective employee and references addressed 'to whom it may concern' will not be accepted unless they can be confirmed directly with the referee.
- Copies of relevant qualifications will be confirmed by requesting sight of certificates, copies of which will be retained on the employees file.
- Curriculum Vitae (CV) will be obtained from all prospective employees. The employment history included on the CV will be tested by taking a reference from a previous employer. This should usually be the most recent employer.
- Request details of any regulatory action or criminal convictions taken against the individual (or the absence of such action) and verify where possible.

For staff recruited for Manager, MLRO or Director positions, the following additional checks will be performed:

- The identity of the prospective employee will be verified by requesting sight of identity verification documents
- Third Party KYC service screening providers
- A police force vetting form

Staff Knowledge, Training and Awareness

Recruiting staff of integrity is not sufficient in of itself. Staff must have sufficient awareness and training to detect money laundering and terrorist financing and to understand what is expected of them.

It is key to effective AML/CFT/CFP arrangements that:

- Staff have sufficient knowledge or awareness to detect money laundering.
- Staff have sufficient training to know how to deal with cases once they know of or suspect money laundering.
- Staff are aware of their personal legal obligations.

The steps adopted by the group to ensure staff have appropriate awareness and training are as follows:

- All new staff will receive AML/CFT/CFP induction training, to include:
 - The provisions of the AML/CFT/CFP code and the appropriate internal procedures and policies including registration and identification procedures, record keeping etc.
 - Their personal obligations under the AML/CFT/CFP Code and associated personal liabilities for non-compliance.
 - The internal reporting procedures detailed in the AML/CFT/CFP Manual.
- AML/CFT/CFP refresher training will be delivered at least annually for all staff and key persons.
- The MLRO will provide other ad hoc information about news and developments. This will be targeted as appropriate.

- The MLRO will send periodic reminders of the need to report certain matters.

Staff promotion and transfer

When an employee is promoted or transferred to a new role the MLRO will be informed in advance, either electronically or in writing. The MLRO will confirm whether any further training or vetting is required, and whether the training or vetting is required before the appointment can take place.

Technological Developments

The Company recognizes the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a consequence:

- The Directors retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the company has engaged with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
- The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

Proceedings

Offences

Any person who contravenes the NOIS / NORUT rules in regard to the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT/CFP) will be reported to The Financial Intelligence Unit of Curaçao.

In determining whether a person has complied with any of the requirements of any part of NOIS / NORUT a court may take account of any relevant supervisory or regulatory guidance which applies to that person and which is given by the Curacao Gaming Authority (CGA).

Appendices

Appendix A | Suspicious Activity Report

Report prepared by:	
Business partners	
Name	
Account ID	
Address	
Email address	
Telephone number	
Is identification and address verification held?	
Is enhanced due diligence held?	

Reason for suspicion	
To include: Identification verification Criminal conduct known or suspected	
Date of report	

Receipt of report acknowledged	
Signed MLRO	
Date	

Approval / Rejections				
Director	Signed		Date	
MLRO	Signed		Date	
Development Review				
Responsible Person Review of Development	Date			
	<i>Review to comment on whether the development has been implemented in accordance with the outlined previously on this Form and whether a further risk assessment should be conducted</i>			
Approved	Director 1 Signed		Date	
	Director 2 Signed		Date	

Appendix B | Banned Countries

- Afghanistan;
- American Samoa
- Barbados
- Belarus
- Botswana
- Burundi
- Cambodia
- Central African Republic
- Cuba
- Ethiopia
- North Korea (DPRK)
- Democratic Republic of the Congo
- Fiji
- Guam
- Iran
- Iraq
- Lebanon
- Libya
- Lithuania
- Mali
- Mozambique
- Myanmar (Burma)
- Nicaragua
- Pakistan
- Palau
- Palestine
- Russia
- Samoa
- Senegal
- Slovakia
- Somalia
- South Sudan
- Sudan
- Syria
- Trinidad and Tobago
- Uganda
- Venezuela
- Yemen
- Zimbabwe

Contested territories that are not internationally recognized:

- Eastern Ukraine,, The Crimea Region (Ukraine), Abkhazia, South Ossetia, Zaporizhzhia, Kherson, Kharkiv, Donetsk, Luhansk People's Republic

Klavitorix BV AML policy Updated v.1.1

Final Audit Report

2026-05-25

Created:	2026-05-25
By:	Millicent Prince (millicent@igatrust.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAGYB3MNL-AZFdgCrI_DI9DKhMnMrmlxlv

"Klavitorix BV AML policy Updated v.1.1" History

 Document created by Millicent Prince (millicent@igatrust.com)

2026-05-25 - 4:07:12 PM GMT- IP address: 161.22.51.16

 Document emailed to Claire Godschalk (Claire@igatrust.com) for signature

2026-05-25 - 4:07:18 PM GMT

 Email viewed by Claire Godschalk (Claire@igatrust.com)

2026-05-25 - 4:10:30 PM GMT- IP address: 104.47.17.126

 Document e-signed by Claire Godschalk (Claire@igatrust.com)

Signature Date: 2026-05-25 - 4:12:07 PM GMT - Time Source: server- IP address: 151.47.128.231 - Signature Appearance Selected: MOBILE_IMAGE

 Agreement completed.

2026-05-25 - 4:12:07 PM GMT