

INVESTAN N.V.

AML, CFT and CFP Policy

Version:	2.0
Last Update:	2024-12-10
Applicability:	Investan N.V.
Owner:	MLRO
Approver:	CEO
Security Class:	Internal

Revision History

Version	Date	Author	Comment
2.0	05.12.2024	MLRO	Policy redefinition
2.0	10.12.2024	CEO	Approval

Table of Contents

1. GENERAL	5
1.1. Purpose	5
1.2. Scope	5
1.3. References	6
1.4. Definitions	7
1.5. Policy Statement	8
1.6. Policy Review and Updates	9
2. AML/CFT/CFP CONCEPTS	10
2.1. Money Laundering and Proceeds of Crime	10
2.2. Financing of Terrorism	11
2.3. Financing of Proliferation of Weapons	12
3. AML COMPLIANCE PROGRAM	13
3.1. Introduction	13
3.2. Basic Elements	13
3.3. Internal Policies, Procedures, and Controls	13
3.4. Money Laundering Reporting Officer (MLRO)	14
3.5. AML/KYC Team	15
3.6. Compliance and Internal Audit Functions	15
3.6.1. Compliance	15
3.6.2. Internal Audit	16
3.7. All Employees	17
3.8. Employee Screening and Training	17
3.9. Regulatory Examination	17
4. RISK-BASED APPROACH	19
4.1. Risk-Based Approach Overview	19
4.2. Business Risk Assessment (BRA)	19
4.3. Customer Risk Assessment (CRA)	19
5. CUSTOMER DUE DILIGENCE	21
5.1. What is Customer Due Diligence	21
5.1.1. Risk-Based Customer Due Diligence	21
5.1.2. Customer Due Diligence Measures	21
5.2. Timing of the Customer Due Diligence Measures	22
5.2.1. Establishment of the business relationship	22
5.2.2. First account review	23

5.2.3.	Ongoing reviews	23
5.2.4.	Termination of the business relationship	24
5.3.	Inability to perform the Customer Due Diligence Measures	24
5.4.	Identification and Verification of the Customer	25
5.4.1.	Initial Identification	25
5.4.2.	Full Identification and Verification	26
5.5.	Identification and Verification of the Beneficial Owner	26
5.6.	Obtaining Information on the Purpose and Intended Nature of the Business Relationship	27
5.7.	Ongoing Monitoring	28
5.8.	Enhanced Due Diligence	32
5.9.	Reliance on Third Parties to Perform CDD	33
5.9.1.	Reliance	33
5.9.2.	Outsourcing	33
5.10.	Funds Management	34
6.	REPORTING	35
6.1.	Unusual Transactions	35
6.2.	Internal Reporting Procedure	36
6.2.1.	Knowledge	36
6.2.2.	Suspicion	36
6.2.3.	Reasonable Grounds to Suspect	36
6.3.	Internal Evaluation and External Reporting	37
6.4.	Actions after Reporting	37
6.5.	Prohibited and Permissible Disclosures	38
6.6.	The Documentation of Unusual Transactions	39
7.	RECORD KEEPING	40
7.1.	Records to be Retained	40

1. GENERAL

1.1. Purpose

The purpose of the Policy is to lay down the Company's approach towards combating money laundering, financing of terrorism and proliferation of weapons of mass destruction. This Policy details the internal practices, measures, procedures and controls relevant to AML/CFT/CFP.

The Policy aims to assist the management and the employees of the Company in understanding and fulfilling their obligations under the state legislation and international treaties, conventions and other legal instruments, thus ensuring an effective implementation of the provisions of all applicable laws, rules and regulations.

The Policy has been issued in order to achieve the following main purposes:

- to provide an understanding of ML/FT/FP threats and risks the Company is exposed to,
- to outline the requirements set out in all applicable laws, rules and regulations,
- to provide an overview of procedures and explain the risk-based approach adopted by the company,
- to explain the duties and responsibilities of senior management, the MLRO and others, including employees, which are relevant to the prevention and detection of ML/FT/FP risks,
- to provide a better understanding of high-risk situations and customers' categories (including PEPs and sanctioned individuals),
- to explain the reporting procedure,
- to explain CDD, monitoring and reporting measures, the timeframe of their application and the approach adopted by the Company,
- to lay down the main principles of the AML/CFT/CFP training program.

1.2. Scope

This Policy applies to the entire Company and all its business activities regulated and licensed by the GCB. The procedures and principles set out herein must be followed at all times by the Company's directors, officers, employees, agents, and assignees. In particular, this Policy applies to third parties engaged by the Company in any player interaction and support activities.

1.3. References

The following sources constitute the main body of the applicable laws and regulations applicable to the Company with respect to AML/CFT/CFP and were used in the development of this Policy:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92),
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99),
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73),
- Sanctions National Ordinance (N.G. 2014, no. 55),
- Kingdom Sanction Act (N.G. 2016, no. 54),
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2),
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29),
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28),
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30),
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34),
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48),
- GCB's Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction,
- FATF and CFATF recommendations,
- Other laws, regulations and other instruments issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law.

1.4. Definitions

“AML/CFT/CFP”	stands for Anti-Money Laundering, Combating Financing of Terrorism and Combating Financing of Proliferation of weapons of mass destruction
“Business Relationship”	means the provision of the gaming services which the Company is licensed to provide to individual customers by the Company
“Beneficial Owner”	in relation to a player account means the individual who ultimately owns or controls the account or on whose behalf a transaction is being conducted through the account
“CDD”	means Customer Due Diligence procedure.
“CRA”	means Customer Risk Assessment
“Customer”	means any physical person aiming to enter a Business Relationship or conduct a single or multiple transaction/s with the company
“Company”	means Investan N.V., a company under the laws of Curacao, bearing company number 153108
“EDD”	means Enhanced Due Diligence, advanced verification measures for high-risk customers and high-risk situations.
“FATF”	means the Financial Action Task Force – the inter-governmental body responsible for setting the international standards for anti-money laundering (AML) and countering terrorist financing (CFT)
“FIU”	means the Financial Intelligence Unit Curacao, the government body principally responsible for investigating and combating ML/FT/FP
“GCB”	means the Gaming Control Board, the gaming regulatory body that licenses and regulates online casinos operating under the laws of Curacao
“ML/FT/FP”	stands for Money Laundering, Financing of Terrorism and Financing of Proliferation of weapons of mass destruction

“MLRO”	stands for the Money Laundering Reporting Officer, the senior compliance manager responsible for the operation of the Company’s AML/CFT/CFP Compliance Program
“Politically Exposed Persons (PEPs)”	means any individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, as well as family members and known close associates of such individuals
“SOF”	means Source of Funds and refers to how the funds used for a particular transaction were obtained by the customer (e.g., transfer from the bank account owned by the customer or someone else, loan, winnings from the other companies)
“SOW”	means Source of Wealth and refers to the origin of the customer’s entire body of wealth (e.g., ownership of the business, employment, investments, inheritance)
“RBA”	means Risk-Based Approach, an approach that allows the Company to allocate resources directed proportionately in accordance with the extent of the ML/FT/FP risks posed, so that the customers posing the highest risks receive the highest attention meeting regulatory needs while effectively combating ML/FT/FP
“UTR/STR”	stands for Unusual Transaction Report / Suspicious Transaction Report

1.5. Policy Statement

The Company recognizes the importance of preventing potential money laundering, financing of terrorist activities and proliferation of weapons of mass destruction, as well as its responsibility to keep financial crime out of gambling.

In order to comply with the applicable laws, the Company intends to do the following:

- 1) To evaluate and address the potential risks associated with ML/FT/FP,
- 2) To develop adequate AML/CFT/CFP policies, procedures, CDD and EDD measures and controls,
- 3) To ensure that the policies, procedures and controls for managing money laundering, terrorist and proliferation financing risks, including the detection of criminal spend, are kept under regular review,
- 4) To perform and/or update the business risk assessment before implementing

any new product, system, control, process or improvement and/or before expanding into new geographical territories, providing new verticals, adopting new funding methods and/or expanding the customer base,

- 5) To adopt a risk-based approach in identifying and mitigating the ML/FT/FP risks,
- 6) To perform an ongoing monitoring of customers' transactions and activities,
- 7) To ensure that any suspicious transaction is brought to the FIU attention, as required by the applicable laws, and that all other appropriate actions are taken to prevent and mitigate ML/FT/FP,
- 8) To ensure that the details of a customer relationship or individual transaction are preserved for eventual assessment by the FIU,
- 9) To develop and implement an AML training program for all relevant employees in the Company.

1.6. Policy Review and Updates

This AML/CTF Policy will be reviewed annually and updated as necessary to ensure it remains effective and aligned with industry best practices and regulatory requirements.

Any changes made to this policy as a result of the review process will be:

- Clearly documented and version-controlled,
- Approved by the CEO,
- Communicated to all relevant stakeholders, including employees, agents, and third-party partners,
- Submitted to the GCB for review and approval,
- Implemented across all relevant business processes and systems.

2. AML/CFT/CFP CONCEPTS

2.1. Money Laundering and Proceeds of Crime

Broadly speaking, the term 'proceeds of crime' or 'criminal proceeds' refers to all property from which a person benefits directly or indirectly, by being party to criminal conduct, for example, money from drug dealing or stolen in a burglary or robbery (this is commonly referred to as criminal property). It also includes property that a person gains by spending the proceeds of criminal conduct, for example, if a person uses money earned from drug dealing to buy a car or a house, or spends money gained in a bank robbery to gamble.

Money Laundering (ML) is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over those proceeds and, ultimately, to provide legitimate cover for their source of income. Failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime a more attractive proposition.

Typically, classic money laundering consists of a number of stages:

- Placement,
- Layering,
- Integration.

Placement is the first stage in the money laundering cycle. The laundering of criminal proceeds is often required because of the cash-intensive nature of the underlying crime (for example, drug dealing where payments are in cash, often in small denominations). The monies are placed into the financial system or retail market or are smuggled to another country. The aim of the money launderer is to avoid detection by the authorities and to then transform the criminal proceeds into other assets.

Layering is the next stage and is an attempt to conceal or disguise the source and ownership of the criminal proceeds by creating complex layers of financial transactions which obscure the audit trail and provide anonymity. The purpose of layering is to disassociate the criminal proceeds from the criminal activity which generated them. Typically, layers are created by moving monies in and out of various accounts and using electronic fund transfers.

Integration is the final stage in the process. It involves integrating the criminal proceeds into the legitimate economic and financial system and assimilating it with other assets in the system. Integration of the 'clean' money into the economy is accomplished by the money launderer making it appear to have been legally earned or obtained.

There is potential for a money launderer to use gambling at every stage of the

process. Although the remote gambling industry might appear less vulnerable as electronic transfers are required for placements, identity theft and identity fraud can enable the money launderer to move criminal proceeds with anonymity. Furthermore, the use of multiple internet transactions can facilitate the layering stage of money laundering.

The Company should be mindful that the offence of money laundering also includes simple criminal spend (the use of criminal proceeds to fund gambling as a leisure activity) and may not include all the typical stages of the laundering process (if any at all). Moreover, criminals and members of terrorist organizations are constantly coming up with new, more advanced and less easy to detect ways of laundering money in an attempt to thwart all efforts to halt such illegal measures.

2.2. Financing of Terrorism

The Financing of terrorism (FT) is the process of making funds or other assets available to support, even indirectly, terrorist activities.

The funding of terrorist activity, terrorist organizations or individual terrorists may take place through funds derived from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organizations and traditional criminal organizations involved in money laundering operations. While the former may thrive on funds derived from legitimate sources, money laundering necessarily involves funds derived from illegal sources.

Another difference is that, while the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds, and avails himself of the profits of crime, the terrorist's ultimate aim is not to generate profit from the fund-raising mechanisms but to obtain resources to support terrorist operations. Thus, in practice, activity from terrorist-funding individuals may be harder to trace, since it will involve lower amounts and less attention-grabbing transactions which do not necessarily appear to be lucrative for the Beneficial Owner in the same way that money laundering activities would.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is often a need for terrorists to obscure or disguise links between the organization or the individual terrorist and their legitimate funding sources. Therefore, terrorists must similarly find ways to process these funds to be able to use them without drawing the authorities' attention.

Financing is required not only to fund specific terrorist acts but, more generally, to meet the operational costs of terrorist organizations, such as maintaining a terrorist network or cell, recruitment and training, sustaining an ideology of terrorism through propaganda, and maintaining an infrastructure of organizational support (even more so if this is to sustain an international network).

2.3. Financing of Proliferation of Weapons

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.

3. AML COMPLIANCE PROGRAM

3.1. Introduction

An anti-money laundering (AML) program is an essential component of the Company's compliance regime. The primary goal of our program is to protect the organization against money laundering and to ensure full compliance with relevant laws and regulations. Our AML program is risk-based and designed to mitigate the money laundering and terrorist financing risks we may encounter. The AML program establishes minimum standards for the organization that are reasonably designed to comply with applicable laws and regulations.

3.2. Basic Elements

Our AML compliance program addresses the following basic elements:

- A system of internal policies, procedures, and controls,
- A designated AML Compliance Officer or Money Laundering Reporting Officer (MLRO) with day-to-day oversight over the AML program,
- An employee screening program and ongoing employee training program,
- An independent audit function to test the AML program

The program ensures that we meet our obligations regarding customer due diligence, reporting unusual transactions, retention periods, data protection, and training. We systematically test and adapt the program to address current risks within our organization. The AML program has the approval of senior management.

The Company must ensure that its foreign branches and subsidiaries, if any, implement AML/CFT/CFP measures consistent with the requirements of the applicable law.

3.3. Internal Policies, Procedures, and Controls

The Company has established policies and procedures, including a clearly expressed commitment to combating the abuse of our facilities and services for money laundering, terrorist financing, and the proliferation of weapons of mass destruction purposes.

Our policies state our intention to comply with current anti-money laundering, combating the financing of terrorism, and financing of proliferation legislation and regulations, particularly the laws and regulations regarding customer due diligence, the reporting of unusual transactions, and keeping adequate records of clients and transactions (NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanction Act).

We have detailed standard AML operating procedures that translate policy into acceptable and workable practices. We also have a process in place to stay current

with regulatory changes.

3.4. Money Laundering Reporting Officer (MLRO)

The Company has formally designated a senior officer at management level, independent of operations, as the Money Laundering Reporting Officer (MLRO). The MLRO is responsible for the detection and deterrence of money laundering and terrorist financing.

The MLRO must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The MLRO must be able to act independently.

Key responsibilities of the MLRO include:

- Designing and implementing the AML program,
- Verifying adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing,
- Reviewing compliance with Company policies and procedures,
- Organizing staff training on compliance-related issues,
- Analyzing transactions and verifying whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions,
- Reviewing all internally reported unusual transactions for their completeness and accuracy with other sources,
- Keeping records of internally and externally reported unusual transactions,
- Executing closer investigation of unusual transactions, if necessary,
- Preparing the external report of unusual transactions,
- Making necessary changes to the AML program,
- Remaining informed on the local and international developments on money laundering and terrorist financing and making suggestions to management for improvements,
- Preparing periodic information on the Company's efforts against money laundering and financing of terrorism and financing of proliferation.

These responsibilities are included in the MLRO's job description, which is signed and dated by the officer, indicating acceptance of the entrusted responsibilities.

3.5. AML/KYC Team

The AML/KYC team acts as a backbone of the Company's AML/CFT/CFP Compliance Program. Its core duty is to implement the AML and KYC policies and

procedures in the day-to-day business operations. This includes, among other activities:

- ensuring that all requirements of the AML policies are correctly applied,
- utilizing systems and controls as appropriate,
- performing identity verification and customer due diligence,
- performing risk assessment and ongoing monitoring of transactions,
- ensuring that the MLRO and any other person who has been assigned with the relevant duties of preventing the ML/FT/FP have complete and timely access to all data and information concerning AML/CFT/CFP activities,
- ensuring proper retention of all transaction records, risk assessments and KYC documents,
- providing practical feedback on the effectiveness of the existing policies and controls,
- assisting the MLRO in the performance of their duties.

3.6. Compliance and Internal Audit Functions

3.6.1. Compliance

The Compliance function is the second line of defense in the detection, prevention and mitigation of ML/FT/FP. The role of Compliance includes the following non-exhaustive list of responsibilities:

- Advising the Company on compliance with requirements emanating from applicable laws, regulations and license requirements,
- Monitoring the controls in place and verifying whether these are being communicated and implemented in practice in an effective and timely manner,
- Identifying any weaknesses in the system,
- Ensuring that the policies and procedures are implemented correctly and as necessary to deal with amendments to applicable laws, regulations and license requirements and to take into account changes to the company's corporate structure, business activities, geographical territories, products and/or services offered, customer base, and any other changes to its setup,
- Acting as the main point of contact and relationship manager with licensing authorities, institutions and bodies in all relevant jurisdictions, including without limitation the GCB.

Any findings and shortcomings noted by the Compliance officers are to be reported to the CEO together with recommendations on mitigation and prevention.

3.6.2. Internal Audit

The Internal Audit function is the third and final line of defense in the Company's AML/CFT/CFP Compliance Program. The following obligations of the Internal Auditor are relevant to the prevention of ML/FT/FP:

- Reviewing and evaluating, at least on an annual basis, in accordance with legal, regulatory and/or license obligations and/or whenever there is a change to the company's corporate structure, business activities, geographical territories, products and/or services offered, customer base and any other changes to its setup, the appropriateness, effectiveness and adequacy of the policy, practice, measures, procedures and control mechanisms applied for the prevention of ML/FT/FP mentioned in the Policy,
- Determining whether the Policy has been effectively implemented in a timely manner, identifying any gaps in the implementation of the Policy and recommending measures for their elimination, prevention or mitigation,
- Setting up strategic audit work programs for Company's operations,
- Presenting reports and making recommendations to the CEO on the company's technical and regulatory compliance and the implementation of the Policy.

Any findings and shortcomings noted by the Internal Auditor are to be reported to the CEO together with recommendations on mitigation and prevention.

Internal audit function is responsible for conducting an audit to evaluate the Company's AML Compliance Program, at least annually, either directly or by employing a third-party auditor. This audit should include:

- Evaluation of AML/CFT manuals
- Customer file reviews
- Compliance management assessment
- Transaction testing
- Assessment of training adequacy
- Evaluation of unusual activity identification systems
- Interviews with employees who handle transactions
- Sampling of unusual transactions
- Review of record retention systems

Audit findings are reported to senior management, with prompt corrective actions required for any deficiencies by a certain deadline.

3.7. All Employees

All Company employees and agents must contribute to the Company's AML/CFT/CFP activities by adhering to these key principles:

- 1) **Awareness:** Improving ML/FT/FP knowledge by participating in the Company-organized training and awareness programs.
- 2) **Compliance:** Adhering to internal AML/CFT/CFP policies, procedures and guidance notes.
- 3) **Vigilance:** Staying alert to potential money laundering or terrorist financing activities in the day-to-day activities.
- 4) **Reporting:** Reporting all suspicious transactions or activities to the MLRO.
- 5) **Confidentiality:** Maintain confidentiality about suspicious activity reports and investigations.
- 6) **Retention:** Properly maintaining records of all transactions and other relevant information, refraining from destroying or altering such records.

3.8. Employee Screening and Training

The Company conducts thorough background checks to screen employees for criminal records. We have developed comprehensive training programs for all personnel who handle transactions that may be qualified as unusual based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions (N.G. 2015 no. 73).

Our training program covers: a) New employees: General training on money laundering, terrorist financing, and reporting requirements b) Front-line staff: Specific training on potential money laundering methods in the industry c) Audit staff: Training on regulatory changes and their impact d) AML Compliance staff: Specialized training on new trends and risk management e) Supervisors and Managers: Higher-level instruction on all aspects of AML/CFT policies and regulations f) Senior management and board of directors: Regular communication on money laundering issues and risks

We maintain detailed records of all training activities, including content, attendees, dates, and assessment results.

3.9. Regulatory Examination

The Company will provide all necessary information and documentation related to our AML/CFT policies and procedures to examiners of the Gaming Control Board upon request. This includes:

- Written and approved AML Compliance Program,
- Records of Business Risk assessment,
- Name and job description of the MLRO,

- Records of reported unusual transactions,
- Records of unusual transactions requiring closer investigations,
- Records of frozen accounts,
- Training schedules and records,
- Internal or external audit reports on AML/CFT policies and procedures,
- Customer files, including risk assessments, CDD, acceptance, and transaction information.

4. RISK-BASED APPROACH

4.1. Risk-Based Approach Overview

The principle behind the Company's AML/CFT/CFP Compliance Program is that resources should be directed proportionately in accordance with the extent of the ML/FT/FP risks posed, so that the customers posing the highest risks receive the highest attention and dedication of resources. In this manner, the application of the risk-based approach should ensure that measures to prevent or mitigate ML/FT/FP are commensurate with the risks identified and that resources are allocated in the most efficient way. High risk areas should be subjected to enhanced controls, whilst simplified or reduced controls may be applied in the areas of low risk.

4.2. Business Risk Assessment (BRA)

The effectiveness of the Company's AML/CFT/CFP Compliance Program depends on the proper understanding of the ML/FT/FP risks to which the Company is exposed.

To this end the Company performs ML/FT/FP Business Risk Assessment (BRA). The purposes of the BRA are:

- Proactively identifying and assessing the risks that money laundering or terrorist financing may occur within the Company's operations,
- Designing and implementing appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks,
- Monitoring and improving the effective operation of these policies, procedures and controls,
- Documenting the Company's risk assessments, including everything that has been done and the reason for this being done.
- The Company's Business Risk Assessment is further described in the **Business Risk Assessment** document.

4.3. Customer Risk Assessment (CRA)

Customer Risk Assessment is an assessment of the particular risks the Company is exposed to in entering into or continuing its business relationship with specific customers, which is based both on the outside information collected on the customer and the history of the Company's business relationship with them.

The information thus collected to draw up the CRA, and the CRA itself, will compose the customer risk profile.

On the basis of the CRA, the proper level of CDD can then be applied, as stipulated in this Policy.

This Policy recognizes three types of customer risk level:

- Unacceptable Risk
- Low Risk
- Medium Risk
- High Risk

Identifying a customer as presenting a high-risk of ML/FT/FP, does not necessarily mean that the customer is involved in ML/FT/FP.

On the other hand, identifying a customer as carrying a lower risk of ML/FT/FP does not mean that the customer presents no risk at all.

In certain situations, the level of risk posed by a customer is Unacceptable, which means that the Company will not establish / terminate business relationship with the customer

More information on the Customer Risk Assessment is provided in the **Customer Acceptance and Risk Assessment Procedure**.

5. CUSTOMER DUE DILIGENCE

5.1. What is Customer Due Diligence

Customer Due Diligence (CDD) is an integral part of the Company's AML/CFT/CFP Compliance Program. It involves gathering information about the customer in order for the Company to assess the extent to which the customer exposes it to money laundering, terrorist and proliferation financing risks.

CDD is intended to allow us to know who our customer is and to build a customer profile on the basis of which we would be able to assess the customer's activity and identify any unusual and/or unexpected behavior. Any such behavior has to be questioned and, if it is found to lead to a suspicion of ML/FT, it also needs to be reported internally to the MLRO and, if required, to the FIU. The documentation and information collected will then assist the authorities in any analysis or investigation of the suspected instance of ML/FT.

5.1.1. Risk-Based Customer Due Diligence

CDD is closely tied with the customer risk assessment performed by the Company. In particular, the level of CDD measures to be applied to a particular customer are risk-based. Depending on the customer's risk level, either standard, enhanced, or simplified CDD measures are applied.

The Company performs standard CDD and standard ongoing monitoring in Low and Medium Risk cases, and EDD and enhanced ongoing monitoring in cases of High Risk. If the customer's risk is Unacceptable, the business relationship with such customer is terminated.

CDD measures also assist the Company to understand the customer's business profile with sufficient clarity to be able to conduct effective risk-assessment and re-assessment.

5.1.2. Customer Due Diligence Measures

The CDD consists of four general activities, as further described in their respective sub-sections below:

- 1) Identification and Verification of the customer's identity,
- 2) Identification and Verification of the (Ultimate) Beneficial Owner,
- 3) Obtaining information on the Purpose and Intended Nature of the business relationship,
- 4) Ongoing monitoring.

In addition, the following activities, while not necessarily being a formal part of CDD, are closely connected to CDD and also form an integral part of the Company's

AML/CFT/CFP Compliance Program. These activities are further described in their respective (sub)sections below and/or in other policy documents:

- 1) PEP screening,
- 2) Sanctions screening,
- 3) Third-Party reliance,
- 4) Termination of the business relationship,
- 5) Retention of CDD records.

5.2. Timing of the Customer Due Diligence Measures

The Company only deals with customers who are individuals and who act in their own name and on their own behalf, whereby all transactions are performed through a dedicated player account opened by each customer with the respective brand operated by the Company.

This is indicative of a relationship that is expected to have an element of duration – even in cases where customer performs a single deposit - and is therefore considered a business relationship between the Company and its customer, as opposed to an occasional transaction.

The Company uses a combination of on-entry, red-flag, and threshold approaches to CDD timing - the so-called hybrid approach. Thus, the player account lifecycle with regards to CDD measures can be represented by the following stages.

The relevant sub-sections below provide more details on how these concepts are implemented for each respective CDD activity, including the information and documents to be collected and the personal details to be verified.

5.2.1. Establishment of the business relationship

The business relationship with a customer is established when the customer successfully opens an account with the Company's casino brand.

The account is considered opened after the perspective customer provides the required personal (registration) details and accepts the Company's Terms and Conditions (which form the legal basis of the business relationship).

At this stage, the following CDD measures are applied:

- personal (registration) details are collected in order to establish the initial customer profile,
- customers are screened for sanctions and PEP status.

5.2.2. First account review

On this stage, the Company completes the main bulk of the CDD activities, namely:

- completes identification and verification of the customer's identity,
- performs identification and verification of the (Ultimate) Beneficial Owner,
- obtains information on the purpose and intended nature of the business relationship,
- carry out the customer risk assessment.

The first account review is performed at the earlier of:

- The legal threshold for customer CDD is reached – the above measures must be conducted when the total accumulated financial transactions reach or exceed **NAf. 4,000**.

The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals made by the customer since the establishment of the business relationship, including any peer-to-peer transfers*.

The threshold also applies to occasional transactions and series of linked transactions which, though individually below the applicable threshold, would cumulatively meet or exceed the threshold.

- Before thirty (30) days have passed since the first deposit into the player account by the customer,
- Before first withdrawal is paid to the customer,
- First ongoing review is triggered.

** peer-to-peer transfers are currently expressly forbidden by the Company's Terms and Conditions.*

5.2.3. Ongoing reviews

Ongoing monitoring consists of account reviews triggered periodically, upon reaching certain thresholds, or when certain events occur. These are:

- before processing a withdrawal (except for low-risk customers),
- when there is a suspicion of ML/FT/FP, regardless of the amount of the transaction or the origin of the suspicion,
- when the cumulative amount of either deposits or withdrawals reaches 10'000.00 EUR or equivalent,
- when there are doubts about the veracity or adequacy of documents or information previously obtained by the Company,
- at other appropriate times to existing customers on a risk-based approach,
- when the Company becomes aware that the circumstances relevant to the customer risk assessment have changed,

- a custom alert, which might be implemented from time to time by the Company, is triggered,
- a change in the customer risk level necessitates additional CDD measures,
- unexpected transaction or a material change in the customer's behavior is detected,
- scheduled reviews – daily (PEPs, accounts under internal investigation*, and other manually scheduled accounts), weekly (high-risk accounts), monthly (medium-risk accounts), every 6 months (low-risk accounts).

** accounts being investigated are usually suspended, however, in some situations account suspension may signal to the customer that an investigation is ongoing (tipping-off) – in these cases the account remains active but is closely monitored.*

5.2.4. Termination of the business relationship

The business relationship with a customer is terminated when:

- the risk level of the customer is classified as “Unacceptable”,
- the Company is unable to complete CDD measures, and
- other cases defined by the applicable laws or the Company's Terms and Conditions.

Where there is no reason for the retention of funds, the funds are to be remitted back to the customer. This has to be done through the same channels used to deposit the funds.

5.3. Inability to perform the Customer Due Diligence Measures

Our Policy states that a customer has to provide all documents within 14 days from the initial request by the Company.

Except as provided below, while CDD measures are carried out, customers are allowed to continue using their gaming account in all respects except for withdrawal of funds, which are blocked. This ensures that the society is protected against ML/FT/FP – since the money can't reach potential perpetrators before the relevant CDD measures are completed.

If the customer still fails to provide the requested documents and/or information to the Company for thirty (30) days following the initial request, the Company will:

- suspend customer account until the request is fulfilled by the customer,
- review the ML/FT/FP risk level of the customer and either allow additional time to fulfill the request or terminate business relationship with the customer - if there are no grounds to suspect ML/FT/FP,
- if there are grounds to suspect ML/FT/FP, an unusual transaction report will

be submitted to the FIU immediately, and the MLRO will wait for the FIU's decision regarding the remaining funds, if any.

The Company must also keep a record of all the attempts made to get the necessary information and documentation.

If the Company is unable to verify the customer's identity after the legal threshold for CDD measures is reached both deposits and withdrawals will be blocked until the customer's identity is verified. Further, if the requested information and documentation is not received within 30 days from the moment the legal threshold was met, the Company shall terminate the relationship with the customer and report the transaction to the FIU.

5.4. Identification and Verification of the Customer

Identification consists in the collection of a set of personal details of the customer. Verification on the other hand consists in confirming the personal details collected for identification purposes through the use of data, information and documentation obtained from independent and reliable sources.

5.4.1. Initial Identification

During the establishment the business relationship (registration if the player account) the following personal details of the customer are collected:

- Name and Surname,
- Date of Birth,
- Permanent residential address,
- Email address,
- Phone number,
- Gender.

The screening against PEPs and Sanctions database commences immediately upon establishing a business relationship (registration). More information on the PEP and Sanctions screening is provided in the **Customer Acceptance and Risk Assessment Procedure**.

A customer must also confirm that his/her age is over eighteen (18), as minors are not allowed to register and/or play. Once registration has been completed, an automatic verification email is sent to a new customer with a link to verify the registered email address. Players who are not registered will not be allowed to deposit funds and/or to play.

In order to corroborate the location of a customer and for ongoing monitoring purposes, the back office constantly checks login IPs, and an automatic alert is raised if the IP-address doesn't match the country of residence or if a customer opens an

account from a high-risk country.

5.4.2. Full Identification and Verification

During first account review the following is performed:

- Additional identification – collection of additional personal details of the customer: place of birth, nationality, and identity number (all except for low-risk customers),
- Identity Verification - actions are taken to verify that the customer exists and is who they claim to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.
- Activity review – personal details check, overview of the financial activity and playing behavior for signs of ML/FT/FP or fraud,
- Confirmation of the payment method ownership and BIN Country match via payment service provider (PSP) back office,
- Check of the IP logs for inconsistent logins and checks for possible duplicate and/or linked accounts.
- Customer risk assessment – the initial risk assessment is performed, and a risk rating is assigned to the customer. More information on the Customer Risk Assessment is provided in the **Customer Acceptance and Risk Assessment Procedure**.

The documents and sources used for verification purposes and the relevant requirements are listed in the **Verification Guidelines**.

5.5. Identification and Verification of the Beneficial Owner

Although our Terms and Conditions state that we only allow customers to register an account, play and transact on their behalf, there is always a risk that a customer can open an account for a third party.

In these circumstances, “Beneficial Owner” of the account means the individual who ultimately controls the nominal customer’s use of the Company’s services or on whose behalf a transaction is being conducted. This could be a single individual or a syndicate that includes one or several customers. In such circumstances, where the funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners, and the Company would therefore have to identify them and verify their identity.

In order to decide on what actions and what documents we need to request from a customer to verify the beneficial owner, it is important to understand the reasons and the circumstances surrounding such accounts, and the risk level involved. To

this end, the following measures are taken:

- Requesting additional
- Requesting additional clarifications from a customer,
- Testing the customer's knowledge of the markets and games they interact with,
- Requesting additional documents from the customer and from a beneficial owner (ID, proof of address and proof of payment ownership),
- Search in the customer database across all brands to identify previous accounts or links,
- Reassessing the ML/FT/FP risk level of the customer,
- Advising customer to use the account only for himself/herself,
- Termination of business relationship in cases where we believe that the registered account holder is not in control of the account and/or the risk level is otherwise unacceptable,
- Submitting an UTR where appropriate suspicion of ML/FT/FP exists.

In the unlikely event that a legal entity is considered to be the Company's customer, the Company will take reasonable steps to verify the identity of the beneficial owner of such entity, using information or data that was obtained from a reliable source. At the minimum identification information, verification and evidence must be gathered for all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer. Where no natural person is identified under the items mentioned above, the natural person who holds the position of senior managing official should be identified.

5.6. Obtaining Information on the Purpose and Intended Nature of the Business Relationship

One of the requirements of CDD is for subject persons to understand why a prospective customer is seeking to acquire a specific service or product from them. The purpose behind the opening of a gaming account is usually self-evident. Customers want to open an account to play.

However, it is important to develop a customer business and risk profile to be able to detect any activity which is considered unusual for a customer in the course of a business relationship.

To this end the Company will perform following:

- Establish the customer's Source of Wealth,
- Establish the customer's expected level of activity,

- Analyze the customer's deposit patterns – usual amounts, frequency of deposits, preferred payment methods,
- Check logins and IP to ensure that they are consistent and match the customer's registered location,
- Perform a background check – social media, online search and other public sources,
- Analyze communication with the customer to see if there are indications of suspicious behavior.

Such a profile helps to identify situations when a customer's behavior or activity is unusual or not in line with the established profile. At that point the customer's risk has to be revised again, and additional documentation has to be requested if necessary.

Source of Wealth (SOW) is the origin of the customer's entire body of wealth (e.g., ownership of a business, employment, inheritance, investments). Taking into consideration the risk-based approach, the extent of the information that the Company collects to verify SOW of a customer varies. In low-risk cases, a declaration, a background check on social media and the average profile of customers from a particular jurisdiction may be sufficient. In high-risk situations the information needs to be supplemented by documentation and data obtained from reliable independent sources.

5.7. Ongoing Monitoring

The ongoing monitoring is performed in two aspects:

- 1) Ongoing monitoring of identity - this ensures that the Company at all times holds accurate and up-to-date identification data of its customers. The documents and information held by the Company may become outdated if the customer's identity changes or the relevant documents expire. In cases when the documents held on file reach their expiry date, there is a notification in place to request new documents from the customer. The validity of the documents and the accuracy of the information held on file are verified during the regular account reviews performed within the ongoing monitoring process.
- 2) Ongoing monitoring of transactions – this is executed to scrutinize customer transactions in order to prevent involvement of the Company with ML/FT/FP. Where we notice that a customer's activity is not in keeping with what we know or expect from the customer (e.g., activity cannot be justified on the basis of a customer's SoW or not in keeping with the average profile or account activity noted to date or activity does not reflect a customer's usual transactional patterns), customer is asked to provide explanation and, where necessary in terms of the risk level, to provide SOF evidence to establish the source of the funds used for that transaction.

Source of Funds (SOF) relates to how the funds used for a particular transaction

were obtained by the customer. As long as a transaction falls within the profile of the customer and the regular or expected activity carried out through one's account, there is no need to obtain specific information and documentation on the same. Should a particular transaction present a departure from the known or expected behavior of the customer, the Company is required to question the same. It is crucial to understand the reason for such divergence and obtain sufficient information and documentation on the matter.

When a customer account is reviewed during the ongoing monitoring, the risk profile of the customer is reassessed to assign a new risk level, if required – based on the newly obtained or observed documents and information.

Moreover, in situations presenting higher risk of ML/FT/FP, SoF is to be requested from time to time even though there may not be any changes in pattern or activity conducted by the customer. Thus, for instance where the amounts deposited by a customer are particularly large, even if these amounts may be in line with the customer profile, we are still obliged to carry out enhanced ongoing monitoring to meet our obligations under the law. This includes obtaining information and documentation on both SOW and SOF.

The Company has implemented various alerts and reports to monitor customers' accounts, and the manual reviews performed on customer accounts are both triggered by such alerts and performed on schedule.

Below is a non-exhaustive list of activities and circumstances that can trigger account review if detected during the ongoing monitoring:

1) Amount and Volume of Transactions

- The transactions or the size of the transactions requested by the customer do not comply with his/her usual practice and activity,
- Large volume of transactions,
- Spike in the volume of transactions,
- A customer with high deposit amounts, having a residential address showing that the customer lives in low-cost accommodation with no known source of income but nonetheless is spending money well above their apparent means,
- The business relationship involves only one transaction, or it is of a short duration,
- Any transaction that, owing to its nature, size or frequency, appears to be unusual,
- Multiple deposits with unusual deposit amount e.g., 27 EUR,
- A lot of deposit attempts with amounts decreasing till a successful deposit is made, followed by attempts with an increasing amount,
- Increase in failed financial transaction attempts,
- Noticeable changes in the gaming patterns of a customer, such as when the

customer carries out transactions that are significantly larger in volume when compared to the transactions, he/she normally carries out.

2) Deposit / Withdrawal

- Deposits have been received from unknown or non-associated third parties of the customer,
- Transfer of funds to and from countries or geographical areas which do not apply or apply inadequately FATF's recommendations on ML/FT/FP,
- Deposit without play activity and leave for a period of time (for instance several months),
- Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling. For instance, suspicions should be raised by any large amounts deposited in gambling accounts that are then cashed out or withdrawn after very little game play or gambling,
- Withdrawal has been requested to a new and unverified payment method,
- A customer who has paid money from one source and asks specifically if it can be paid back to another source would raise immediate questions concerning both money laundering and fraud.
- Customers make frequent deposits and withdrawal requests without any reasonable explanation.

3) Verification / Communication

- A customer is reluctant to provide complete information when establishing a business relationship,
- A customer provides unusual or suspicious identification documents that cannot be readily verified,
- A customer's registered details seem to be incomplete or incorrect,
- Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g., previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc.),
- Unwillingness to communicate with the customer support staff,
- A customer is asking a lot of questions about KYC, verification, account screening etc.,
- Customers who wish to end the relationship after receiving the Company's request to provide CDD information, or who are otherwise uncooperative regarding the CDD process,

- Customers who provide the same address or telephone number as another customer, with whom they do not appear to have a connection.

4) Betting / Playing Behavior

- A customer exhibits unusual gambling patterns with an almost guaranteed return or very little financial risk. It is accepted that some customers prefer to gamble in this way but, in some instances, the actions may raise suspicion because they are different from the customer's normal gambling practices.
- A customer regularly gambles large amounts of money and appears to find a level of losses acceptable. In this instance, the customer may be spending the proceeds of crime and sees the losses as an acceptable consequence of the process of laundering those proceeds.
- Betting on new markets or new betting pattern behavior (e.g., substantial change in stake amount, change to different product-from Sport to Casino).

5) Account Re-activation

- Account has been activated after a period of non-activity and personal details have been changed (change of name, email address or phone number, IP address from a new place, IP changing all the time and showing different parts of the country or different countries in a short period of time).
- Re-activation of inactive users with substantial balances or sudden increase in bets placed by means of a user that has been inactive over a long period.

6) Customer's profile

- Activity not justified on the basis of a customer's source of wealth or not keeping with the average profile.
- There is negative publicity implicating the customer with crime, terrorism or organizations linked to terrorism.
- The customer has links to a jurisdiction or area where terrorists are active, or which are known to sympathize or support terrorists or terrorist organizations.
- Transactions in which payments are made with funds originating in tax havens, countries or territories that do not cooperate in the fight against money laundering, terrorist and proliferation financing, or in states where there is knowledge of the existence of particularly active criminal organizations.
- Customers where there are indications that they act on behalf of others, seeking to hide the identity of the actual customer.

- Customers who have the status of or are related to politically exposed persons (i.e., persons who perform or have performed significant public functions in another country).
- Customers with published police or criminal records or linked to persons prohibited from trading or to terrorist financing activities.
- Customers attempt to register more than one account with the same brand.

5.8. Enhanced Due Diligence

Enhanced Due Diligence (“EDD”) is applied whenever the Company identifies any high-risk situations or high-risk customers. EDD entails taking more stringent steps in the application of CDD as well as requesting more detailed information on SOW and SOF. These EDD measures include:

- 1) All standard CDD measures, described above, including documentary evidence of SOW/SOF,
- 2) Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.,
- 3) Obtaining additional information on the intended nature of the business relationship and the reasons for intended or performed transactions,
- 4) Researching in additional independent, reliable sources to verify information provided or made available to the Company:
 - local or open-source information, such as press reports,
 - checks against Law Enforcement, Adverse Media, Financial Datasets.
- 5) Taking additional measures to understand better the background and financial situation of the customer:
 - Online and media search – Instagram, Facebook and other social media platforms to build the customer’s profile, including looking at available photos online regarding customer’s occupation, hobbies and activities.
 - Internet search on the customer’s name, email address and phone number. The information could be useful to see whether the customer’s name is linked to another person’s identity or to some negative publicity, illegal activities etc.
 - Google Map search – in order to check the address, registered in the account and evaluate the financial situation of the customer.
- 6) Increasing the monitoring of the business relationship (enhanced ongoing monitoring), including greater scrutiny of the transactions.

5.9. Reliance on Third Parties to Perform CDD

5.9.1. Reliance

The applicable law allows the Company to rely on third parties for the performance of its obligations regarding identifying the customer and verifying their identity, the identity of the beneficial owner, and the purpose and intended nature of the business relationship. Such third parties would have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the Company. There are certain legal requirements applicable to such situation.

The Company does not rely on third parties for its CDD activities and does not intend to enter into any such scenario.

5.9.2. Outsourcing

This is different to the outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the Company, in accordance with its procedures, and is subject to the delegating Company's control of the effective implementation of those procedures by the outsourced company.

However, the decision whether to on-board a customer or to continue a business relationship on the basis of risk cannot be outsourced.

Further, the Company remains responsible at all times for compliance with the applicable laws. Any activity performed by an agent or group company is to be considered as an activity performed by the Company. As such, any customer on-boarded by the agent or group company has to undergo the same checks and controls as customers on-boarded by the Company itself.

Service provider's activities under the outsourcing arrangement shall be periodically reviewed for quality and consistency with the legal requirements and the outsourcing contract, both quantitatively as well as qualitatively.

5.10. Funds Management

The Company tries to mitigate the risk of ML/FT/FP by only using payment methods that are offered by regulated and reputable financial institutions.

In addition, the Company will never allow players to either deposit or withdraw cash.

All funds deposited by the player will be credited to the player's corresponding player account.

Additionally, in order to mitigate ML/FT/FP risks, where possible, upon a withdrawal request or termination of the business relationship, the Company shall use a "closed loop policy" policy and thus the Company will only remit withdrawals to the same account from which the customer's funds originated.

There could be payment methods that do not process withdrawals, as well as other

circumstances preventing the Company from applying the “closed loop” policy. In the event that the Company is unable to remit the funds to the same source through the same channels, inevitably new payment details will have to be requested from the customer. In the event that these details give rise to suspicion, the MLRO is required to submit an UTR and suspend the remittance pending the FIU expressing its decision regarding the account balance.

6. REPORTING

The Company understands that Unusual (Suspicious) Transactions reporting has to be considered as one of the most important AML/CFT/CFP obligations, and the Company is fully committed to ensure that any unusual transactions and activity are brought to the FIU's attention without delay.

The Company will make every effort to ensure that all employees understand their responsibilities and obligations related to the prevention of ML/FT/FP and know when and how they have to report their suspicions and what actions to take and/or refrain from taking following such reporting.

6.1. Unusual Transactions

The definition of an unusual activity and transaction as well as the types of transactions indicating ML/FT/FP is very broad. A suspicious transaction will often be inconsistent with the normal business relationship patterns of the specific account.

The Company shall ensure that it maintains adequate information and knows enough about its customers' activities in order to recognize on time that an activity, a transaction or a series of transactions are unusual or suspicious. The Company will pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

The following transactions and activities must be generally considered unusual and subject to the reporting obligations:

- 1) Presumed money laundering transactions or terrorist financing, i.e. such transactions where there is cause to presume that they can be related to money laundering or terrorist financing
- 2) Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55),
- 3) Transactions in the amount of NAf. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 - A cashless transaction in the amount of NAf. 5,000 or more.
 - A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the customer.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the customer
 - Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits

- A cash-out in the amount of NAf. 5,000 or more.
 - Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000.
- 4) Suspicions that funds are proceeds of criminal activity,
 - 5) Suspicious activity that may be connected to a possible ML/FT/FP, or a customer with negative publicity linked to ML/FT/FP, even if there are no unusual transactions in the account,
 - 6) Suspicious activity of prospective customers (e.g., a person has registered an account with us, but never deposited and therefore has not activated the account, while doing an online search, we find out that this person was accused of ML or had confirmed links to TF – even if the business relationship has not been established, we need to report such instances as a suspicious activity),
 - 7) Any transactions connected to FATF / CFATF “black-listed” countries (“High-Risk Jurisdictions subject to a Call for Action”), including pending transactions or any requests to establish a business relationship.

6.2. Internal Reporting Procedure

By law we are required to report to the GCB when we have knowledge, suspicion or reasonable grounds to suspect ML/FT/FP or that funds (regardless of the amount involved) are proceeds of criminal activity. Below is an explanation of these three concepts.

6.2.1. Knowledge

Having knowledge means actually **knowing something to be true**. In case the MLRO or any other employee is aware or is in possession of information of ML/FT/FP activities, the MLRO should immediately proceed with filing a report with the GCB.

6.2.2. Suspicion

Suspicion of ML/FT/FP is more subjective than knowledge and in order to determine its existence, we need to rely on objective criteria. **Suspicion** is a **possibility**, which is more than fanciful, **that the relevant facts exist**.

6.2.3. Reasonable Grounds to Suspect

The requirement to file a report goes beyond “suspicion” and also includes the obligation to report when “reasonable grounds to suspect” exist. This implies that a further obligation to report arises where, on the basis of objective facts or

circumstances, a reasonable person would have inferred knowledge or formed the suspicion that ML/FT/FP existed or that funds were the proceeds of criminal activity.

The MLRO is responsible to ensure that all of the Company's employees:

- are aware of the Internal Reporting Procedure,
- understand its importance and the consequences of their failure to report,
- know, where to find an Internal Concern Report template and other supporting information and
- know how to avoid a "Tipping Off" offence.

To this end, the MLRO must conduct a periodic internal AML/CTF training for all relevant employees and also monitor the day-to-day compliance of the relevant employees with the Internal and External Reporting Procedure.

Any suspicions about ML/FT/FP must be reported directly to the MLRO. This will ensure confidentiality and enhance the speed of reporting. Therefore, when an employee becomes aware or gets a suspicion about ML/FT/FP, he/she must treat such instance with the utmost urgency and shall report the matter to the MLRO without delay. It is expected that the internal report has to be submitted as soon as reasonably possible, but not later than the next working day after the employee becomes aware of the information or matter that has risen to his/her suspicion.

6.3. Internal Evaluation and External Reporting

It is the responsibility of the MLRO to receive and evaluate all Internal Concern Reports and report to the GCB any transaction or activity that, after their evaluation, they know or suspect, or have reasonable grounds to know or suspect, may be linked to ML/FT. Such reports must be treated with the utmost urgency and submitted to the GCB **on the same day** when knowledge or suspicion of ML/FT/FP is considered to subsist by the MLRO.

The decision to file or not to file an UTR must **always be the MLRO's/designated employee's own** and should not be subject to the direction or approval of senior management of the Company.

6.4. Actions after Reporting

After the successful submission of the Report to the FIU, an acknowledgement with the external reference number is received, which needs to be filled in into the "Internal / External Concern Reports" spreadsheet for future references.

While waiting for a reply from the FIU the following procedure will be in place:

- 1) In case it was decided to maintain the business relationship with the customer in question, the customer will be considered as a high-risk customer and enhanced ongoing monitoring will be performed. The MLRO will analyze

transactions and activity and consider whether it is necessary to submit the Additional Information File and/or Transaction Report to the FIU.

- 2) All upcoming requests from the customer will be treated with careful consideration in order to avoid the “Tipping Off” offence. The circulation of the information related to the External Report shall be limited internally only on a “need to know” basis to avoid risks of leakage and disclosure.
- 3) The MLRO shall consider seeking advice from the FIU prior to carrying out drastic measures with regards to the account, as any unjustified action may alert the customer to the fact that he is being suspected or investigated (e.g., termination of business relationship or delay in processing withdrawals or imposing additional restrictions).
- 4) The Company shall follow the FIU instructions regarding the execution of the transaction(s) through the account.

6.5. Prohibited and Permissible Disclosures

The Company, its directors, officers and employees are prohibited to disclose to the person concerned or to a third party that:

- An UTR has been made to the FIU,
- The FIU, GCB or another government body requested information within the context of an ML/FT/FP analysis,
- Information has been given to the FIU, GCB or another government body within the context of an ML/FT/FP analysis,
- An ML/FT/FP analysis or investigation has been, is being or may be carried out by the FIU, GCB or another government body.

Breach of the above constitutes a criminal offence and, given the potential prejudice that any disclosure of the above-mentioned information may have on an analysis or investigation, it arises even though no prejudice may actually result or the person disclosing the information did not know or suspect that the disclosure was likely to prejudice the analysis or investigation.

Additionally, the performance of CDD measures by the Company may also tip off the customer. Therefore, the MLRO shall decide, on a case-by-case basis, if and how to continue the CDD process. If the MLRO reasonably believes that performing the CDD process will tip off the customer, it may choose not to pursue that process and should file an UTR to the FIU.

6.6. The Documentation of Unusual Transactions

The Company shall maintain registration with the FIU and maintain access to the goAML reporting portal after validation by the FIU.

The MLRO must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Company shall report to the FIU the details of the transactions by means of the goAML reporting portal.

The reports and the submission of the thereto related information (all supporting documents) should be done in English.

7. RECORD KEEPING

The Company must retain records of any business relationship it enters into and of any transaction it carries out. These records are to include any documentation and information produced or obtained in complying with our obligations.

The main purpose of keeping records is to:

- Show our compliance with the obligations at law,
- Assist the Company in revising its AML/CFT/CFP policies and procedures, especially in revising its Business Risk Assessment,
- Ensure effective ongoing monitoring,
- Assist the FIU, relevant supervisory authorities and law enforcement agencies in the prevention, detection, analysis or investigation of possible ML/FT/FP.

7.1. Records to be Retained

The following records must be maintained:

- All records on all transactions (both domestic and international), with the level of detail sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.
- All records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents),
- Account files and business correspondence with the customer,
- Internal Concern Reports made to the MLRO, including internal evaluations and determinations made by the MLRO and the reasons for not filing an UTR with the FIU,
- UTRs submitted by the MLRO.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority

The Company must maintain these records for a period of at least five (5) years after the business relationship with the customer has ended (or an occasional transaction has been performed, as the case may be).

However, in some cases the FIU or other competent have the right to demand those records be retained for a longer period when this extension is considered necessary for the purposes of the prevention, detection, analysis and investigation of ML/FT/FP activities by the competent authorities.