

DIGIBET N.V.

Groot Kwartierweg 10, Curaçao

AML/CFT MANUAL

May 2025

Table of Contents

<u>DEFINITIONS AND ABBREVIATIONS</u>	<u>3</u>
<u>1. AML/CFT POLICY</u>	<u>5</u>
1.1 POLICY	5
1.2 FINANCING OF TERRORISM	5
1.3 OBJECTIVE.....	6
1.4 SCOPE	6
<u>2. REGULATORY FRAMEWORK</u>	<u>7</u>
2.1 NATIONAL REGULATIONS	8
2.2 INTERNATIONAL REGULATIONS	9
<u>3. THE RISK BASED APPROACH</u>	<u>10</u>
3.1 BUSINESS RISK ASSESMENT BRA.....	11
3.2 CUSTOMER RISK ASSESMENT	12
3.3 RISK SPECIFIC FACTORS IN GAMBLING SECTOR.....	13
<u>4. POLICIES, PROCEDURES AND CONTROLS</u>	<u>14</u>
4.1 PROCEDURES.....	15
4.2 RISK MANAGEMENT.....	15
4.3 KYC.....	17
<u>5. DUE DILIGENCE</u>	<u>18</u>
5.1 ENHANCED DUE DILIGENCE	19
5.2 SIMPLIFIED DUE DILIGENCE	21
<u>6. THE MONEY LAUNDERING REPORTING OFFICER</u>	<u>24</u>
<u>7. INDEPENDENT TESTING POLICY FOR AML/CTF POLICIES AND PROCEDURES PURPOSE</u>	<u>33</u>

8. CONSEQUENCES OF NON COMPLIANCE.....34

Definitions and Abbreviations

Account Holder:	an individual who applied and was granted an account held
	at the internet gateway operated by the Company for the use of the provided Services.
AML:	Anti Money Laundering. All efforts focused on the prevention of transforming proceeds obtained from criminal activities into funds which appear to be obtained from legal activities.
CFT:	Combating the Finance of Terrorism. All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
The Company	DIGIBET NV., a limited liability company under the laws of Curaçao, registered with the Chamber of Commerce of Curaçao under number 158812.
FATF:	Financial Action Task Force (www.fatf-gafi.org)
FIU:	Financial Intelligence Unit.
KYC:	Know Your Client
MLRO:	Money Laundering Reporting Officer
Non-reputable Jurisdiction:	Country mentioned on the list of the FATF as jurisdictions for which a call of action has been issued or are mentioned on the list of monitored jurisdictions.

Player:	Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which an account has been opened providing him/her with a unique code.
Player Account:	an account granted to an individual after registration.
The	account is created and issued by the Company and is required for wagering with real money. Only one Player Account is permitted per person, per family and per Shared Environment.
Shared Environment:	an environment that has a common internet connection which includes but is not limited to airplanes, households, universities, libraries, cyber cafes, coffee shops and work forces.
Service:	the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.
Website	the website www.betnbet.com which is operated by the Company.
Contact:	info@digibetnv.com

1. AML/CFT Policy

1.1 Policy

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 the process of making dirty money look clean. Money Laundering consists of three phases: Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits; Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities; Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

1.2 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 of funds, FT is mostly concerned with obscuring the end recipient of the funds.

7 1.4 What is 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.

1.3 Objective

The Company is a limited liability company, duly incorporated and registered in accordance with the laws of Curaçao. This policy is written based on the national legislation on AML, CFT and the penalization of predicate crimes of Curaçao and applicable international standards set by the FATF. Combined these regulations provide a solid, internationally accepted standard for the procedures maintained for the prevention of the misuse of the Services provided by the Company.

Proper Identification of Account Holders, verification of the identity, monitoring of Player activities and reporting of unusual activities are part of the measures the Company has in place in an effort to prevent, deter or mitigate industry related risks.

1.4 Scope

The Company is committed to the highest national and international AML and CFT standards when providing its Services and requires management and employees to follow these standards.

2. Regulatory Framework

The Regulations for combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass Destruction (ML/FT/FP) are an integral part of the land-based and the online gambling license requirements for the Curaçao jurisdiction.

These Regulations are issued in implementation of:

- article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92) and;
- article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99);
- Sanctions National Ordinance (N.G. 2014, no. 55); Kingdom Sanction Act (N.G. 2016, no. 54).
- With these Regulations, the GCB offers the casinos a guideline to promote compliance with the laws and decrees with regard to money laundering, financing of terrorism and financing of proliferation and to implement sound internal policies and procedures to combat Money Laundering and the Financing of Terrorism. These include among others:
 - 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);
 - 5 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 Nation's 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 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).

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

2.1 International regulations

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting International standards by regularly implementing these standards in its national legislation.

On international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing

necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Although Curaçao is not a EU member, the Company, in addition to the FATF rules, where applicable, adheres to AML rules issued in directives by the European Union. Subsequently the present policy is a combination of the FATF, EU and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

3. The Risk-based Approach

At our company, compliance with anti-money laundering (AML) obligations is a core priority. As part of our commitment to maintaining the integrity of our operations, we apply a Risk-based Approach in line with the Financial Action Task Force (FATF) Recommendations.

What the Risk-based Approach Means to Us

We recognize our responsibility to implement and maintain a comprehensive AML compliance program designed to prevent money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. Our program is built around the principles of the Risk-based Approach.

By adopting this approach, we ensure that the measures we take to prevent or mitigate these risks are proportionate to the level of risk identified. Specifically:

- Where higher risks are identified, we implement enhanced measures to manage and mitigate those risks;
- Where lower risks are identified, we may apply simplified measures, provided these remain consistent with our overall obligation to counter money laundering and terrorist financing threats.

Our Commitments under the Risk-based Approach

As a casino operator, we are committed to the following actions in applying the Risk-based Approach:

1. **Risk Assessment:** We assess the risk of money laundering and terrorist financing occurring within our operations. This includes evaluating all relevant risk factors such as:
 - Customer profiles,
 - Geographic locations,
 - Products and services offered (types of games of chance),
 - Delivery channels.
2. **Policy and Control Design:** Based on this assessment, we design and implement appropriate internal policies, procedures, and controls to effectively mitigate

the identified risks.

3. **Monitoring and Review:** We continuously monitor the effectiveness of our AML policies and controls and make improvements when necessary.
4. **Documentation:** We document all risk assessments and decisions, including the rationale behind each action taken.

Additionally, we take into account the findings of the National Risk Assessment (NRA) in the jurisdictions where we operate, and we integrate these insights into our own internal risk assessments.

We understand that risks are dynamic, and as such, we regularly review and update our Risk-based Approach to ensure it remains effective and responsive to emerging threats. This ongoing commitment reflects our dedication to maintaining compliance and protecting the integrity of our operations.

Business and Customer Risk Assessments

As a licensed and regulated casino operator, our company is fully committed to implementing a comprehensive and effective Risk-Based Approach (RBA) to combat money laundering (ML), terrorist financing (TF), and the financing of the proliferation of weapons (FP). A fundamental element of this approach is the conduct of both a Business Risk Assessment (BRA) and a Customer Risk Assessment (CRA). These assessments allow us to identify, evaluate, and mitigate the risks we face in the course of our operations.

3.1 Business Risk Assessment (BRA)

In line with regulatory obligations and FATF Recommendations, we conduct a Business Risk Assessment to identify the ML/TF/FP risks inherent to our operations. This assessment allows us to ensure that our internal policies, controls, and procedures are not only appropriate but also proportional to the risks identified.

Our Business Risk Assessment includes:

- An analysis of how our services could be exploited for money laundering, terrorist financing, or proliferation financing.
- A thorough consideration of risk factors, including:

- Types of customers we serve,
- Products and services offered (e.g., games of chance),
- Delivery channels,
- Geographic risks.

We also incorporate the findings and recommendations of the National Risk Assessment (NRA) into our evaluation process.

Based on the outcome of the BRA, we establish a clear risk appetite, defining the level of risk we are prepared to accept. This informs our broader Anti-Money Laundering Compliance Program and helps us align our mitigation strategies accordingly.

Ongoing Review and Documentation

- The BRA is reviewed at least annually or more frequently if there are changes in:
 - Our operational environment,
 - Business model (e.g., new markets, payment methods, or games),
 - Regulatory requirements.
- The full assessment is documented and approved by the Board of Directors, and is made available to the Gaming Control Board (GCB) upon request.
- The documentation includes:
 - The methodology used,
 - Justification for each risk rating (low, medium, or high),
 - Information sources consulted,
 - Overall results and conclusions.

3.2 Customer Risk Assessment (CRA)

In addition to the BRA, we carry out a Customer Risk Assessment for each player, either before establishing a business relationship or when conducting an occasional transaction. This assessment helps us evaluate the specific risks associated with individual players and informs the level of Customer Due Diligence (CDD) to be **applied**.

Key Elements of the CRA:

- The CRA identifies and categorizes ML/TF/FP risk as low, medium, or high.
- Based on the CRA, we determine the appropriate level of CDD measures, which are outlined in our Customer Acceptance Policy (CAP).

Our Customer Acceptance Policy (CAP) includes:

- Identification of customer types likely to pose higher-than-average risk,
- Risk indicators used to classify players (low, medium, high),
- Criteria for determining when to decline or discontinue services,
- Provisions for enhanced measures in relation to Politically Exposed Persons (PEPs) and Sanctions Screening.

As the customer relationship evolves, the CRA may be re-evaluated and updated to reflect changes in customer behavior, transactions, or other relevant factors.

3.3 Risk-Specific Factors in the Gambling Sector

Our risk assessments are specifically tailored to reflect the unique characteristics of the gambling industry. We identify four main risk categories:

1. Customer Risk

We evaluate the ML/TF risk arising from individual customers. Higher risk may be indicated by:

- Multiple or irregular income sources,
- PEP status,
- Use of third parties to place bets or cash out winnings,
- High spenders with unverifiable source of funds,
- Tourists or casual players with unusual transaction patterns,
- Use of multiple player accounts to obscure activity,
- Unknown customers attempting to redeem large sums of chips,
- Use of junket operators.

We define thresholds for what constitutes typical transaction values and monitor deviations accordingly.

2. Geographic Risk

We assess the risk posed by a customer's nationality, residency, and source of funds.

Heightened geographic risk is associated with:

- Jurisdictions with weak AML/CFT systems,
- Countries subject to international sanctions,
- High-corruption jurisdictions,
- Countries known for terrorist activity or inadequate financial oversight.

We consult reliable international sources including:

- FATF's lists of High-Risk Jurisdictions,
- U.S. Department of State, OFAC, and CFATF reports,
- Transparency International's Corruption Perception Index.

We maintain and update a list of high-risk and low-risk countries to guide our CRA process.

4. Policies, Procedures, and Controls

To effectively manage and mitigate the risks identified in both our BRA and CRA, we have established robust internal policies, procedures, and controls, including:

1. Customer Due Diligence (CDD) protocols;
2. Record keeping practices compliant with legal requirements;
3. Suspicious transaction reporting procedures;
4. Risk management measures, including:
 - Customer Acceptance Policies (CAP),
 - Customer Risk Assessment procedures,
 - Internal control systems,
 - Compliance oversight and communication strategies,
 - Regular employee training and screening programs.

All such measures are documented, implemented company-wide, and approved by the Board of Directors. Their effectiveness is monitored on an ongoing basis, with enhancements introduced where necessary, especially in cases involving high-risk

indicators.

By integrating these structured assessments and controls into our operations, we ensure our continued compliance with regulatory standards and uphold our commitment to the integrity of the gaming industry.

4.1 Procedures

In an effort to be compliant with the applicable rules, regulations and international standards, the Company has procedures in place to which it attains itself to when providing Services to Account Holders. These procedures cover the following standards:

- **Customer Due Diligence**
 - Know Your Client
 - Due Diligence
 - The Money Laundering Reporting officer
- **Risk Management**
 - Risk Classification
 - Monitoring of Account Holder activities
- Reporting of unusual transactions
- Recordkeeping

4.2 Risk Management

Risk Classification

The Company maintains a risk-based approach in relation to its clients in order to effectively detect and deter any risks it may be exposed to such as money laundering,

the financing of terrorism or any prohibited transaction such as fraud.

The Company maintains the following risk classification:

- Low risk
- High risk

Low risk

All Players are classified as Low risk and are subjected to Standard Due Diligence procedures related to the request for KYC documentation as per the process described above and constant monitoring of activities on the account.

High Risk

The Player activity is the determining factor for the classification of a Player as High Risk. Any Player of which an automated alert has been generated or an inappropriate activity has been detected will be categorized as High Risk, for which an Enhanced Due diligence procedure is applied. The instances in which a High risk classification is assigned includes but are not limited to those Customer Due Diligence

4.3. Know Your Customer (KYC)

Identification & verification

Following international standards and local applicable legislation, it is imperative for a company to know its clients. A sound KYC policy and procedure are critical in protecting the safety and soundness of a company and the financial system. In line herewith the Company has the following procedures in place.

KYC information request / Identification of the player

An individual cannot participate in a game for money unless that individual has registered and has been provided with a Player Account. Only one Player Account is permitted per person, per family and per Shared Environment.

To be registered as a Player, an individual must register personally and submit the following KYC information:

- date of birth together with valid identification showing that he/ she is over eighteen
- (18) years of age or the applicable legal age of majority as stipulated in the jurisdiction of your residence. Identification documents which must be submitted include copy of a valid Passport, copy of other identification paper and a proof of address (not older than 3 months);
- Player's first and last name;
- Player's full residential address;
- Player's valid email address;
- payment details; and
- a username and a password

On registration, a geographical location check is carried out on the applicant's computer IP to ensure that person is in a permitted jurisdiction. If the applicant is not in a permitted jurisdiction, he/she will not be allowed to continue the registration process. The Company proceeds to review the information provided and

may request additional documentation in order to verify the provided information. The Player Account may be put on hold until satisfactory information has been received or terminated if the Company finds the information contained in the Player Account to be false or misleading. The Company reserves the right to refuse to open or close a Player Account at its own discretion following review of the provided KYC information.

Log in details

It is not permitted for a Player to share the login details to access the system with a 3rd party. The Company reserves the right to cancel, without refund, a Player Account if the login details were disclosed to a 3rd party.

5. Due Diligence

Standard Due Diligence

The Company requests the following information to verify the identity of the Player:

1. A driver's license or valid passport;
2. A recently (not older than 3 months) issued copy of a utility bill or bank statement

Standard Due Diligence is conducted in the following cases:

- anytime during the Player onboarding;
- upon a request for withdrawal;
- when a threshold of a cumulative withdrawal of 2,000 € or equivalent is reached in 30 days
- anytime at the discretion of the Company.

The Company further reserves the right to conduct a phone verification of the Player Account to verify details provided by the Player at the time of registration or at any other time requested by the Company. The details include but are not limited to name, home address, email of the registered Player Account holder, phone number, photo ID, payment methods, bet types, amounts and event details. Failure to satisfactorily complete this verification due to the previously provided details being fake, false, incorrect, misleading, non-existing, not belonging to the Player or unable to be verified, may result in the Company closing the Player Account and the confiscation of any winnings.

Enhanced Due Diligence

5.1 Enhanced Due Diligence (EDD)

As part of our commitment to a fully compliant Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) framework, our company applies a **Risk-Based Approach** to customer due diligence. In cases where the risks of money laundering (ML) or terrorist financing (TF) are assessed to be higher, we implement **Enhanced Due Diligence (EDD)** measures.

EDD is a critical component of our compliance program and ensures that we apply a **proportional and targeted level of scrutiny** where the risks warrant a higher level of control and oversight.

When EDD is Applied

We conduct Enhanced Due Diligence in all instances where elevated ML/TF risk is identified. This may include, but is not limited to, situations involving:

- Customers who are **residents of high-risk geographic areas**;
- **Transactions or products** that may promote anonymity;
- **Political Exposed Persons (PEP's)**
- **New products, services, or business practices**, including:
 - New delivery channels,
 - New or developing technologies, whether used for new or existing offerings.

Measures Taken Under Enhanced Due Diligence

The level and nature of due diligence applied are always consistent with the **specific risk factors identified**. In high-risk scenarios, we intensify both our **monitoring and information-gathering efforts** to detect unusual or suspicious activities.

Examples of Enhanced Due Diligence measures include:

- **Collecting additional information about the customer**, such as:
 - Occupation,
 - Previous residential addresses,
 - Information available via public databases or open-source internet searches.
- **Gathering details on the intended nature and purpose** of the business relationship.
- **Obtaining evidence of the source of funds or source of wealth**, which may include:
 - Salary or wages,
 - Pension payouts,
 - Property or asset sales,
 - Dividends or share sales,
 - Gambling winnings,
 - Inheritance or gifts,
 - Legal compensation payments.
- **Requesting information on the rationale** behind specific or intended transactions.
- **Requiring senior management approval** before:
 - Establishing a relationship with a high-risk customer,
 - Continuing a relationship when increased risk indicators arise.
- **Conducting enhanced, ongoing monitoring** of the customer relationship and associated transactions.
- **Ensuring the origin of funds passes through a bank or financial institution** that is subject to similar Customer Due Diligence standards.

Ongoing Monitoring in High-Risk Cases

Where a customer or activity presents a **continuing elevated risk**, we are required to periodically request **updated source of funds information**—even if the customer’s behavior or activity patterns appear consistent. This ensures we maintain a clear and up-to-date understanding of the legitimacy of their financial activity.

Our Enhanced Due Diligence measures are designed to safeguard our operations and align with both international standards and local regulatory expectations. These procedures form a key part of our wider effort to **prevent the misuse of our services for financial crime** and uphold the integrity of the gaming sector.

In certain specific instances the Company will conduct Enhanced Due Diligence by requesting the following KYC information:

1. A driver’s license or valid passport;
2. A selfie of the Player holding the identification document;
3. A recently issued (not older than 3 months) utility bill or bank statement
4. A bank statement showing the initial deposit;
5. A bank statement no older than 3 months from the bank to which a withdrawn amount should be deposited;
6. Information regarding the source of wealth.

- **Politically Exposed Persons (PEPs)**

At Digibet we recognize the heightened risk associated with doing business with Politically Exposed Persons (PEPs). In line with applicable legal and regulatory obligations, we have established and implemented robust procedures to identify and manage such relationships appropriately.

- **Definition and Scope**

A **PEP** is an individual who is or has been entrusted with a prominent public function. This includes, but is not limited to, heads of state, senior politicians, senior government officials, judicial or military officials, senior

executives of state-owned corporations, and important political party officials. The same level of scrutiny applies to:

- Foreign PEPs;
- Domestic PEPs;
- Individuals entrusted with prominent roles in international organizations;
- **Family members and close associates** of PEPs.

- **Obligations in Relation to Foreign PEPs**

When a foreign PEP is identified as a customer or beneficial owner, **[Company Name]** undertakes the following measures in addition to standard Customer Due Diligence (CDD):

a. Risk Management Systems

We maintain **appropriate risk-management systems** to proactively identify whether a customer or beneficial owner is a politically exposed person. PEP screening is conducted at the onboarding stage and repeated regularly during the course of the business relationship.

b. Senior Management Approval

Before entering into or continuing any business relationship with a PEP, we are required to obtain **prior approval from senior management**. This includes:

- Establishing a relationship with a new PEP customer;
- Continuing a relationship with an existing customer who has become a PEP;
- Conducting occasional transactions involving a PEP.

Senior management includes individuals responsible for directing day-to-day operations or, in some cases, the designated Compliance Manager.

c. Source of Wealth and Source of Funds

We are required to take **reasonable measures** to establish and verify the **source of wealth and source of funds** of the PEP. This process includes:

- Collecting a signed statement from the player;
- Verifying information through **reliable, independent public sources**;
- Where public sources are inadequate, requesting **supporting documentation** from the customer.

d. Enhanced Ongoing Monitoring

All business relationships involving a PEP are subject to **enhanced ongoing**

monitoring. This includes closer scrutiny of transaction patterns, customer behavior, and updates to the individual's PEP status.

- **Domestic PEPs and International Organization PEPs**

For domestic PEPs and individuals with prominent roles in international organizations, **[Company Name]** takes **reasonable measures** to determine their status. Where a higher risk is identified, we apply the same enhanced measures outlined above (approval, verification of funds and wealth, and ongoing monitoring).

- **Risk-Based Approach to PEPs**

While enhanced due diligence is required for all PEPs, the **intensity and scope of measures** are determined using a **risk-based approach**. This allows us to tailor our compliance actions according to the individual's level of exposure, jurisdiction, political prominence, and transaction behavior.

- **Screening and Ongoing Monitoring**

PEP screening is conducted:

- **At onboarding**, as part of our standard due diligence process;
- **On an ongoing basis** during the business relationship.

If a customer who was **not initially identified as a PEP** becomes one during the course of the business relationship, we will:

- Apply the appropriate enhanced measures;
- Complete these actions **within 30 days** of becoming aware of the change in status.

Failure by the customer to comply with requests for documentation or verification within this time frame will result in the **termination of the business relationship**.

At **Digibet NV**, we maintain a zero-tolerance approach toward unmanaged PEP risk. Our compliance team ensures all such procedures are documented, auditable, and reviewed regularly in line with regulatory expectations.

5.2 Simplified Due Diligence (SDD)

As part of our Risk-Based Approach to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF), our company applies **Simplified Due Diligence (SDD)** measures in situations where the **risk of money laundering or terrorist financing is assessed to be low**. These measures are proportionate to the nature and level of the lower risk and are always implemented in line with applicable regulations and guidance.

When Simplified Due Diligence is Applied

SDD is only applied **after a formal risk assessment** concludes that the customer, product, service, or transaction presents a **low risk of ML/TF**. SDD **must not** be applied in any case where:

- There is a suspicion of money laundering or terrorist financing,
 - A higher-risk factor is identified,
 - Enhanced Due Diligence is required.
-

Examples of Simplified Due Diligence Measures

In line with regulatory guidelines and internal policy, the following SDD measures may be applied in low-risk situations:

- **Limiting the information collected:** If the risk level is demonstrably low, only core personal identification details may be required (e.g., name, date of birth, nationality), as outlined in Section III.2.1.
- **Delaying verification:** In specific cases, the **verification of identity** (of both the customer and any beneficial owner) may be completed **after** the business relationship is established.
- **Adjusting verification methods:** In low-risk scenarios, verification may be performed using **alternative, reputable information sources**, including those that may not contain a photographic ID, provided the source offers sufficient reliability.

- **Limiting the scope of personal data verification:** While basic identification details must always be verified, the extent of verification of additional personal data may be reduced, provided we are confident that we understand who the customer is.
- **Reducing the frequency of updates:** The requirement to regularly update customer identification and verification details may be relaxed, depending on the duration and nature of the relationship.
- **Lower levels of ongoing monitoring:** In low-risk cases, we may reduce the **intensity and frequency of transaction monitoring**, with monitoring thresholds adjusted according to a reasonable monetary benchmark.

Maintaining Compliance and Control

Although Simplified Due Diligence allows for reduced obligations in clearly low-risk cases, our casino remains fully committed to maintaining visibility and oversight. We continuously ensure that:

- All SDD measures are **justified and documented** based on a thorough risk assessment;
- We maintain the **flexibility to escalate to Standard or Enhanced Due Diligence** if circumstances change;
- SDD **is never applied** when there are grounds for suspicion or when risk indicators shift.

By carefully calibrating our customer due diligence efforts according to risk, we can allocate resources effectively while continuing to **protect our operations against financial crime** and ensure **regulatory compliance**.

Enhanced Due Diligence is applied as soon as a Player is classified as a High risk including but not limited to the following situations and as further discussed in the section 'Monitoring of Account Holder activities:

- a) if the Player is a national of a High-Risk Country, or the geographical location check at onboarding shows that the Player is residing in a Non-reputable or High-Risk Jurisdiction;
- b) upon suspicion of a Player attempting to or having created multiple Player Accounts in multiple different names;
- c) upon suspicion of Player(s) being part of a syndicate of Players colluding to gain an advantage over the Company;
- d) upon suspicion of the Player being a politically exposed person (PEP);
- e) at the detection of any irregular, suspicious, inappropriate or fraudulent activity;
- f) anytime, at the discretion of the Company.

If the Company is not able to verify the identity of the Player based on the provided documentation and further efforts, the Company reserves the right to put the Player Account on hold pending the provision of verification information, or to terminate the account if it finds the information contained in the Player Account to be false or misleading.

6. The Money Laundering Reporting Officer (MLRO)

The Company has designated an MLRO who is in charge of the review of KYC information and the monitoring of Player Account activities. Specifically, the MLRO is in charge of the following:

- Ensure a proper review of the Player Accounts by the personnel in relation to identification and verification of an Account Owner,
- Keep a list of registered Account Holders;
- Monitor the reviews and investigations conducted by the designated

personnel performed on the Player Account activities;

- Provide initial and ongoing training to all relevant staff ensuring awareness of their personal responsibilities and the procedures in respect of identifying Players, monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions;
- Cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity;
- Ensure that this policy is adhered to, reviewed and maintained regularly.

- **The Monitoring of Account Holder activities**

Designated personnel will conduct the reviews and the monitoring of the Player Accounts and will further conduct investigations in case any irregular activities are detected.

Security technology are in place generating automated alerts which are thereafter thoroughly investigated by the department.

The presence of any irregular, suspicious, inappropriate or fraudulent activity or any attempt thereto, will cause the pertaining Player to be classified as High risk for which EDD procedures are implemented.

Player accounts are reviewed and monitored for the presence of any of the following situations:

- the provision of fake, false, incorrect, misleading, non-existing, KYC information which do not belong to the Player or are unable to be verified;
- provision of fictitious names such that the true beneficial owner is not known;
- the detection of inappropriate play and/ or fraudulent activity;
- the detection of irregular Player activity including but not limited to the placing of zero- risk or even bets;
- complex or large transactions or groups of transactions which are likely, by their nature to be related to money laundering or the funding of terrorism
- upon suspicion of a Player attempting to or having created multiple Player Accounts in multiple different names;
- upon suspicion of Player(s) being part of a syndicate of Players colluding to gain an advantage over the Company;
- at the detection of any irregular, suspicious, inappropriate or fraudulent activity;
- anytime, at the discretion of the Company
- fraudulent or unlawful use of the system by Players, in an attempt to break into or otherwise circumvent the security measures set up by the system;

- The use of any software program endowed with Artificial Intelligence;
- attempt to log in from a Non-reputable Jurisdiction or a High Risk Jurisdiction.

Specific attention is paid to the following instances:

- **Multiple accounts**

Only one Player Account is permitted per person, per family and per Shared Environment. If more than one Player Account is created per person, house, building, mailing address, phone number, IP address, family, Device or Shared Environment then all related Player Accounts will be closed. No winnings, refund nor deposits will be paid out. Family includes, but is not limited to, parents, partners, spouse, children, siblings and close relatives.

If the suspicion arises that multiple Player Accounts have been created in multiple different names or that a Player Account is a part of a syndicate of Players colluding to gain an advantage over the Company, the Company will proceed to suspend all suspicious Player Accounts pending an investigation. The investigation will consist of the review of playing history, IP location histories including VPN and proxy databases and action to delay ratios commonly displayed with computer sharing technology. If the Company concludes from the investigation that an Account Holder or a group of Account Holders have created multiple accounts and are playing as part of a syndicate of Players, the Company will proceed to withhold any cash or bonus winnings and reserves the right to withhold deposited funds.

Whenever an Account Holder requests for a withdrawal of funds from his/ her account, the system will check the presence of multiple accounts and further checks whether the Account Holder has used a false proxy. At the presence of multiple accounts, all the accounts will be closed, and the Account Holder will be denied the opening of a new account.

- **Unusual activities**

If an Account Holder has unusual deposits and gets flagged by the system, the Company will perform an investigation in which the Account Holder may be requested to provide further information. The Company will suspend the account until further documentation is in place. If the Account Holder has not provided satisfying information within 30 days, the account will be terminated. The MLRO will proceed with the reporting of the unusual transaction to the relevant authority.

- **Withdrawal or Pay out of funds**

The Company has established the following procedures with regards to the withdrawal or pay out of funds.

Request for withdrawal

Withdrawal requests must be made from a Player Account. Withdrawal requests sent by any other means of communication will not be processed. Upon receipt of a request for withdrawal, the Company will request KYC documentation verifying the identity of the Player.

The Company will not deposit withdrawn funds to another source from which it was originated. If for any reason this is no longer possible, the Company will request additional verification documentation evidencing the details and ownership of the new withdrawal method.

Transfers or pay outs will only be made to the Player. Transfers to third parties are not permitted.

- **Prior review of account activity**

Before processing any withdrawals, the Company will conduct additional review of the Player Account for any irregular activity such as money laundering or suspicious play such as:

- the placement of a deposit without having placed any bets, or only to receive free spins. A Player must have always placed at least his deposit amount in bets

before proceeding to withdraw the funds;

- the possible creation of multiple Player Accounts in multiple different names;
- possible collusion between Players.

Upon the occurrence of any of the instances mentioned above, the Company may decide to withhold funds and proceed to further request EDD documentation or conduct further investigation and resolve to:

- suspend the Player Account until receipt of sufficient verification information, where still applicable;
- immediately block the access of a Player to the system or to his/ her account and seize all funds held in the account;
- close or terminate a Player Account and seize all funds held in such account,

Followed by the report of the activity to the relevant authority as further described below.

- **Transactions using Cryptocurrency**

Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency. Following this transaction all transactions (deposits, wagers and payout) with the Player must be conducted using the same crypto currency as with the first deposit.

The Company will at no time sell/buy/exchange crypto currency with and/or to FIAT currency. The Company is bound by the following requirements as set by the Master License Holder:

- Collect and verify proof of identity and proof of address as described above in the '**Client Due Diligence**' paragraph and to make sure that a Player is over 18 years of age;
- Collection and storage of hardware KYC in all pathways from signup, login, deposits and withdrawals, including but not limited to IP address, mac address and browser information to ensure that all wagering, deposits and withdrawals are to/from the same Player (IP and computer);
- The Company will make available to the Master License holder on demand and provide proof of balance as acceptable by the Master License Holder, to ensure Player's funds have been deposited;
- Provide proof of Solvency to the Master License Holder on a periodic basis (weekly, monthly) to ensure that operator has all funds to cover all bets and jackpots and that the crypto currency is kept in a separate account.
- The Company will display the rate of exchange from crypto currencies to FIAT currency on the home page of the Website. In no way shall the Company make exchanges between any crypto currency and any FIAT currency.
- The Company must include in their Terms and Conditions and highlights that crypto currency values can change dramatically depending on the market value.

It is important to note that due to the current anti-money-laundering regulations, the Player may deposit money into the Player Account only in order to play and to use the Services. Likewise, the Player may only withdraw winnings and **not** the funds deposited into the Player Account. Players who deposit and withdraw without gaming activities will have their funds blocked until further notice. The Company is not a financial institution and does not grant interest on deposits. In any case, the Company reserves the unlimited right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Notification of new payment methods will be made on the homepage of the Website and sent by e-mail to the Account Holders as they are added. For each new depositing method, this Manual and the Terms and Conditions on the Website will be updated accordingly.

- **Security review**

The Company reserves the right to conduct a review at any time to validate the identity, age and/or registration data provided by the Account Holder in order to verify the use by the Customer of the provided services for any breach of the Terms and Conditions and any applicable laws. At the moment of registration the applicant provides the Company with authorization to make any relevant inquiries pertaining to his person and to use and disclose information to any third party considered necessary in order to conduct its verification checks. Third party agencies may be engaged in an effort to confirm the provided age, identity, address and payment details, the ordering of a credit report and/ or the verification of the provided information by checking it against certain public or private databases. All applicant/ Account holders are made aware that by accepting the Terms and Conditions of the Company, they agree that the provided information may be used, recorded and disclosed and that the data may be recorded by the Company or third party engaged. The review may be performed from time to time at the discretion of the Company and/or due to regulatory, security or other business reasons,

During the review the Customer may be restricted from withdrawing funds from the account and/ or prevented from accessing certain Services offered on the website.

- **Reporting of unusual transactions**

Any transactions or circumstances for which the Company has not received sufficient verifying information for and/or of which the Company knows, suspects or has reason to suspect that any of the transaction(s), among other actions, (i) involve funds derived from illegal activities, (ii) are intended to conceal funds from illegal activities, or (iii) involve the use of the Company system to facilitate criminal activity, may give rise to its report to the FIU in Curaçao. The Money Laundering Reporting Officer (MLRO) is in charge of the reporting with the relevant authority and will hold a list of all instances in which it did not consider it necessary to report. The decision not to report will be sufficiently supported.

- **Recordkeeping**

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables investigating authorities to identify a satisfactory audit trail for individual transactions including the amounts, currencies and type of transactions.

In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

- **Staff Due Diligence-**

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates, which are checked and verified by the Company's Human Resources Department.

7. Staff Training Policy on Regulatory Compliance and AML/CTF

Purpose:

This policy ensures that all employees of the company are appropriately trained and

equipped with the knowledge and skills necessary to comply with anti-money laundering (AML), counter-terrorist financing (CTF), and internal regulatory requirements.

Key Principles:

- **Mandatory Induction Training:**
All new employees must complete a mandatory AML/CTF compliance training program within the first 30 days of employment.
- **Annual Refresher Training:**
All staff members must participate in an annual refresher course, which includes updates on legislative changes, emerging threats, and any changes to internal procedures.
- **Targeted Training:**
Staff members in high-risk departments (e.g. payments, VIP account management, fraud and risk teams) receive specialized, role-specific training tailored to their exposure to AML/CTF risks.
- **Knowledge Evaluation:**
Following each training session, staff must complete a knowledge assessment. Failure to pass the test will result in repeat training.
- **Documentation and Tracking:**
All training sessions and attendance records are documented in a central training register and are available for review by regulatory authorities upon request.

8. Independent Testing Policy for AML/CTF Policies and Procedures

Purpose:

This policy establishes the framework for independent testing and validation of the company's AML/CTF compliance program. The objective is to ensure the effectiveness and integrity of the systems, controls, and processes in place.

Key Principles:

- **Annual Independent Audit:**
An internal or external party, independent from daily compliance operations, must conduct an annual review of:
 - AML/CTF framework,

- Customer due diligence (CDD, EDD, SDD),
- Internal controls and monitoring systems,
- Staff training and reporting procedures.
- **Findings and Recommendations:**
A formal audit report must be prepared following the review, including:
 - Identified weaknesses or non-compliance issues,
 - Risk-based recommendations for remediation or improvement.
- **Corrective Action Plan (CAPA):**
Management is responsible for preparing and implementing a clear Corrective and Preventive Action Plan in response to audit findings, including specific timelines and responsible persons.
- **Board Oversight:**
The audit report and corrective plan are presented to the Board of Directors for review and approval. The Board ensures appropriate follow-up and accountability.
- **Record-Keeping:**
All audit reports, action plans, and related documentation must be securely retained and made available to competent authorities upon request.

9. Consequences of Non-Compliance

As a licensed and regulated gaming operator, **[Company Name]** is fully committed to maintaining compliance with all applicable Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and regulatory obligations.

Non-compliance with this policy—whether by action, omission, or negligence—will be treated with utmost seriousness. The following consequences may apply:

1. Regulatory Action

Failure to comply may result in enforcement measures by regulatory authorities, including:

- Financial penalties;
- Revocation, suspension, or restriction of gaming licenses;
- Imposition of special supervisory measures or independent audits;
- Public warnings or reputational sanctions.

2. Legal Consequences

Depending on the severity of the breach, the company may be exposed to:

- Civil liability;
- Criminal proceedings or prosecution;
- Freezing or seizure of assets;
- Restrictions on its ability to contract with financial institutions or payment providers.

3. Reputational Damage

Non-compliance can severely impact the company's brand, including:

- Negative media exposure;
- Loss of trust among customers, partners, and stakeholders;
- Barriers to entering or operating in new or existing markets.

4. Financial Loss

Non-compliance may lead to:

- Direct costs such as fines, legal fees, and penalties;
- Indirect costs such as revenue loss, higher compliance costs, and loss of commercial relationships.

5. Operational Disruption

Failure to meet compliance standards may result in:

- Suspension of services;
- Disruption to banking or payment processing;
- Increased scrutiny by regulators and third parties.