

AML-CTF-CPF POLICY AND PROCEDURES

Contents

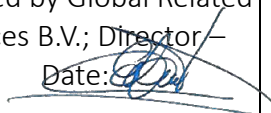
1	INTRODUCTION	3
1.1	POLICY STATEMENT	3
1.2	WHAT IS MONEY LAUNDERING?.....	3
1.3	WHAT IS THE FINANCING OF TERRORISM?	3
1.4	WHAT IS PROLIFERATION OF WEAPONS OF MASS DESTRUCTION?	4
1.5	THE NEED TO COMBAT MONEY LAUNDERING AND FINANCING OF TERRORISM	4
1.6	THE AML REQUIREMENTS FOCUS ON THE FOLLOWING AREAS:	4
1.7	PROCEEDS OF CRIME.....	4
2	PURPOSE.....	5
3	DEFINITIONS	7
4	POLICY IMPLEMENTATION	8
4.1	RESPONSIBILITY OF SENIOR MANAGEMENT	8
4.2	DISTRIBUTION OF THE AML POLICY.....	8
4.3	APPOINTMENT OF THE COMPLIANCE OFFICER	8
4.4	REPORTING STRUCTURE AND INDEPENDENCE	9
4.5	DUTIES OF THE COMPLIANCE OFFICER	9
5	BUSINESS RISK ASSESSMENT.....	10
6	CUSTOMER RISK ASSESSMENT	10
7	CUSTOMER ACCEPTANCE POLICY	11
7.1	AGE VERIFICATION.....	11
7.2	TARGETED FINANCIAL SANCTIONS.....	11
7.3	COUNTRIES AND TERRITORIES EXCLUDED FOR REGISTRATION	12
7.4	ACCEPTED PAYMENT METHODS	13
7.5	NO CASH POLICY.....	13
8	CUSTOMER DUE DILIGENCE	14
8.1	SIMPLIFIED DUE DILIGENCE (SDD).....	16
8.1.1	ENHANCED DUE DILIGENCE	16
8.1.2	POLITICALLY EXPOSED PERSONS (PEPs)	17
9	ONGOING MONITORING.....	20

9.1	SCRUTINY AND MONITORING OF TRANSACTIONS:.....	20
9.2	FRAUD MANAGEMENT	21
10	REPORTING PROCEDURES AND OBLIGATIONS.....	22
10.1	INTERNAL REPORTING PROCEDURES	22
10.2	EXTERNAL REPORTING PROCEDURES.....	23
10.3	PROHIBITION OF DISCLOSURE.....	23
11	RECORD KEEPING PROCEDURES	24
12	AML COMPLIANCE PROGRAM	25
12.1	COMPLIANCE OFFICER	25
12.2	EMPLOYEES	25
12.3	TRAINING.....	26
12.4	INDEPENDENT AUDIT FUNCTION	27
12.5	EXAMINATION BY THE GAMING CONTROL BOARD.....	27
13	REGULARITY OF POLICY UPDATES	28

Document Information:

Approval	Board of Directors
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	April 10, 2025
Next Review Date	May 30, 2026

Version History:

Date	Version	Summary Changes	Approved by Management
April 10, 2025	2.0	Policy update in line with CGA Regulations	Approved by Global Related Services B.V.; Director – Date:  30 May 2025

1 INTRODUCTION

1.1 Policy Statement

Final Enterprises N.V. (the Company), being established in and governed by the laws of Curaçao, is committed to implementing robust policies to prevent money laundering (ML), terrorism financing (TF), and proliferation financing (PF). In light thereof, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (AML/CTF/CPF) policy. Adherence to this Policy is obligatory and vital for guaranteeing that the Company remains in full compliance with relevant laws and regulations pertaining to AML/CTF/CPF. As a responsible gaming enterprise operating in Curaçao, we acknowledge the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

1.2 What is Money Laundering?

Generally, money laundering is described as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds. This process is of crucial importance for criminals as it enables the perpetrators to make legitimate economic use of the criminal proceeds. When criminal activity generates substantial income, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or to the persons involved. Criminals do this by disguising the sources, changing the form or moving the funds to a place where they are less likely to attract attention.

Traditionally, three stages were identified for the process of money laundering – the placement stage, the layering stage and the integration stage.

- a) Placement: the first introduction of the cash proceeds of criminal conduct into the financial system, especially via deposit-taking institutions and, again, particularly in jurisdictions with extensive banking secrecy laws and little or no anti money laundering legislation.
- b) Layering: separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
- c) Integration: the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the financial system.

1.3 What is the Financing of Terrorism?

Financing of terrorism is the process by which terrorist organizations or individual terrorists are financed in order to be able to carry out acts of terrorism.

The financing of terrorist activity, terrorist organizations or individual terrorists may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Funds coming from legal sources is a key difference between terrorist organizations and traditional criminal organizations involved in money laundering operations. Another difference is that while the money launderer generates income by obscuring the link between the crime and the generated funds, the terrorist's ultimate aim is not to generate income from the fund-raising mechanisms but to obtain resources to support terrorist operations.

1.4 What is Proliferation of weapons of mass destruction?

Proliferation of weapons of mass destruction (WMD) is defined as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials. Proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing.

1.5 The Need to Combat Money Laundering and Financing of Terrorism

The Company has three main concerns:

1. Reputational Risk;
2. Regulatory Risk; and
3. Litigation Risk.

1.6 The AML requirements focus on the following areas:

- a) Identification procedures;
- b) Record Keeping;
- c) Internal procedures;
- d) Staff Education, Training and Development;
- e) Internal controls and communication procedures that are appropriate for the purposes of forestalling and preventing money laundering and the financing of terrorism; and
- f) Procedures, controls and evaluation.

1.7 Proceeds of Crime

Irrelevant of how money is transferred to any of our casinos, there is always a risk that this money would have originated from illegal activities, such as credit/debit card fraud, theft from the player's employer or even narcotics trafficking. Hence, by paying greater attention and increasing monitoring of high spenders, the Company will be able to mitigate this risk.

2 PURPOSE

Incorporated and having its statutory seat in Curacao the Company is bound by the local legislation with regards to Anti-Money Laundering, Countering Financing of Terrorism and Proliferation of Weapons. The local authority in charge of the supervision on AML- CFT matters for the gaming sector is the Curacao Gaming Control Board.

The following legislation is applicable to the Company and needs to be taken into consideration within this policy and procedures:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- 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);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th 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 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 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);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);

- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

The Company checks for amendments to all Decrees and Regulations on a regular basis and updates the policies and procedures accordingly to meet any such changes. Besides these regulatory authorities, the Company also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering ('FATF'), the Caribbean Financial Action Taskforce (CFATF).

3 DEFINITIONS

CFATF means the Caribbean Financial Action Taskforce. An organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Compliance Officer means a senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.

Customer Due Diligence or **CDD** means the process of identifying and verifying customers and assessing their risk.

FATF means the Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations means a framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions means deposits and withdrawals (bonusses are not included). Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

FIU means the Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

Kingdom Sanctions Act means the National Ordinance also known as the "Rijkssanctiewet", published under N.G. 2016 no. 54.

NOIS means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Money Laundering or **ML** means the process of disguising the illicit origin of funds.

Politically Exposed Persons or **PEPs** means individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Sanctions National Ordinance means the National Ordinance also known as the "Sanctielandsverordening", published under N.G. 2014 no. 55.

Source of Funds refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of Wealth means the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

Terrorist Financing or **TF** means providing funds for terrorist activity or organizations.

Unusual transaction means a transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

Ultimate beneficial ownership or **UBO** means the natural person who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

4 POLICY IMPLEMENTATION

Policy implementation employs a risk-based approach to detect and mitigate risks related to money laundering (ML), terrorist financing (TF), and proliferation financing (PF). This approach encompasses the following key components: Business Risk Assessment, Customer Risk Assessment, Customer Acceptance Policies, Due Diligence Procedures, Ongoing Monitoring, and Reporting Mechanisms. Detailed processes and responsible departments are outlined in the subsections below.

4.1 Responsibility of Senior Management

Senior Management is responsible for the following:

- Setting and approving the overall principles of the Policy for the Prevention and Combatting of Money Laundering and Terrorist Financing.
- Appointing a Compliance Officer and Deputy Compliance Officer and communicating the internal policies to them.
- Defining the duties and responsibilities of the Compliance Officer.
- Ensuring that effective systems and controls are in place for compliance with all applicable rules and regulations.
- Ensuring that the Compliance Officer has timely access to all necessary data to effectively perform their duties, including customer identity information, transaction documentation, and other relevant records.
- Ensuring that all employees know to whom they should report any information regarding unusual transactions.
- Ensuring that the Compliance Officer and Deputy Compliance Officer have sufficient resources, including competent staff and appropriate technological tools.
- Assessing and approving the annual report, and taking appropriate actions to address any weaknesses or deficiencies identified within it.

4.2 Distribution of the AML Policy

The Executive Management Team has reviewed and approved this AML Policy. It is distributed to all staff members, including frontline workers, team leaders, managers, and the Board. The Policy is also reissued and redistributed whenever updates are made.

One of the primary responsibilities of the Compliance Officer is to submit a report to the Executive Management Team for assessment at least once every twelve (12) months. This report evaluates the effectiveness of the Policy and its associated operational procedures. Additionally, the Compliance Officer is expected to provide recommendations for potential improvements to operational processes or policies.

The Executive Management Team will conduct a thorough assessment of this Policy at least once every twelve (12) months to identify necessary adjustments or updates. Any recommendations for changes should be directed to the Compliance Officer.

Except for directives from relevant authorities, any proposed amendments to the Policy must be reviewed and approved by the Compliance Officer, the Executive Management Team, and legal counsel.

4.3 Appointment of the Compliance Officer

A suitably experienced senior staff member must always be designated as the Compliance Officer. The designated individual is responsible for ensuring compliance, and their contact information is made accessible to all employees and relevant personnel from service providers.

4.4 Reporting Structure and Independence

The Compliance Officer holds no other position within the organization or any affiliated company or supplier, ensuring independence from all other functions to prevent actual or perceived conflicts of interest.

Under the supervision of the Chief Executive Officer (CEO), the Compliance Officer has the authority to operate independently from other departments to effectively fulfill their specific duties and obligations.

The Compliance Officer receives full and public support from the Executive Management Team in executing their responsibilities. All staff are required to assist the Compliance Officer (or the appointed officer, as appropriate) in fulfilling these duties.

4.5 Duties of the Compliance Officer

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the Company's efforts against money laundering and financing of terrorism and financing of proliferation.

5 BUSINESS RISK ASSESSMENT

The Business Risk Assessment (BRA) framework is a crucial component of Company Name's AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating money laundering, terrorist financing, and proliferation financing risks within the Company's operations.

Company Name performs thorough BRAs, evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed regularly. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment.

6 CUSTOMER RISK ASSESSMENT

The Company adopts a risk-based approach in our AML compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF risks specific to the online gaming industry. When developing its AML compliance program, the Company assesses risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Company may employ simplified measures.

The Company understands that its clients will expose it to different levels of risk depending on the particulars of each client, hence it has established a Framework called Customer Risk Assessment (CRA) to identify such risks per client.

The Company has set up the risk factors applicable to all its current participants (new and existing) in order to identify whose circumstances would indicate higher risk and flag them for enhanced due diligence, including enhanced ongoing monitoring, or refusal/termination. On the basis of the CRA, the Company will be able to apply the proper level of CDD and will be able to identify a customer as presenting a higher risk of ML/FT.

In order to carry out the CRA, the Company should consider the following risk factors:

- a) Customer Risk: Assessing the customer's background, occupation, and transaction patterns. High-risk customers, such as politically exposed persons (PEPs) and those from high-risk jurisdictions, receive particular scrutiny.
- b) Products/Service Risk: This factor evaluates the risks associated with the products and services offered. The following products and services are considered to be at higher risk of criminal exploitation. This includes gaming products or services where customers can influence game outcomes, either on their own or in collaboration with others. Additionally, certain payment methods used by customers and accepted by casinos are seen as riskier for ML and TF.
- c) Geographic Risk: This assessment considers the geographic location of the customer and the transaction, with countries that have weak AML/CFT regulations or high levels of corruption being deemed higher risk. The nationality, residence and place of birth of the player have to be considered as these might be indicative of a heightened geographical risk.

- d) **Delivery Channel Risk:** This factor looks at the risks associated with the methods used to establish a business relationship through which transactions are carried out. The Company considers the increased risk of ML/TF of the use of channels that favor anonymity and interactions on a non-face-to-face basis and, to the extent possible, shall take all reasonable measures to address and mitigate said risks.

7 CUSTOMER ACCEPTANCE POLICY

The Company's general policy is not accepting any players whose funds have emanated from ill-gotten means, and to comply with all applicable obligations in relation to anti-money laundering (AML) and know your customer (KYC). The Company identifies all players prior to establishing a business relationship and proceeds to verify the data provided on certain activities being carried out, which may be first deposit, cumulative deposit thresholds being reached, cumulative withdraw transactions exceeding Naf. 4000 (or the equivalent in another currency) or reaching other triggers. Players who are not registered will not be permitted to play for real money. One of the main drivers is to protect our operations from fraudulent transactions. The other key driver is preventing players from being able to launder money using our services; such money-laundering could take the form of either:

- (a) a customer gambling using funds which they have obtained through criminal conduct – proceeds of crime; or
- (b) a customer seeking to disguise the fact that they have obtained money from criminal conduct by passing it through our account in an attempt to 'clean' it.

It is important that the Company has a clear and concise understanding of all customer practices in order to avoid any possibility of money laundering and/or terrorist financing exposure.

To this end, the Company restricts or prohibits the commencement of business relationships with customers and/or entering into transactions that fall outside our established risk appetite.

7.1 Age Verification

The Company will not accept any player unless of legal age, 18 years or older. If there is suspicion of a minor registering a fake date of birth, the account will be closed immediately. If the customer provides satisfactorily a valid ID together with a face ID (clear picture of the customers holding the ID next to his face), the account may be reopened by the COMPLIANCE OFFICER.

7.2 Targeted Financial Sanctions

We are committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with these sanctions. This includes, but is not limited to, the following:

The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.

The Company shall perform perpetual sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:

- At the moment of registration;
- At the moment of withdrawal request;
- At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered, the Company shall immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance,

and shall immediately file a report with the FIU. Once the true match is confirmed by the supervisory authority, the Company shall terminate services and keep the frozen assets until further instruction from the supervisory authority.

7.3 Countries and territories excluded for registration

Below is the general list of banned countries; however, it is not exhaustive and might also include other countries that may have been banned due to various reasons, e.g., change in FATF recommendations, countries banned by license agreements, countries with other deficiencies etc.

- | | |
|--------------------------------------|---|
| 1. Afghanistan | 37. Lithuania |
| 2. Armenia | 38. Kuwait |
| 3. Aruba | 39. Malaysia |
| 4. Australia | 40. Marshall Islands |
| 5. Austria | 41. Martinique (.FR) |
| 6. Belize | 42. Maldives |
| 7. Belgium | 43. Mali |
| 8. Bonaire | 44. Netherlands |
| 9. Bosnia and Herzegovina | 45. North Korea (Democratic People's Republic of Korea) |
| 10. Brazil | 46. Norway |
| 11. Burma/Myanmar | 47. Occupied Palestinian Territory |
| 12. Burundi | 48. Poland |
| 13. Central African Republic | 49. Puerto Rico |
| 14. Curaçao | 50. Qatar |
| 15. Cyprus | 51. Reunion |
| 16. Denmark | 52. Republic of Guinea |
| 17. Democratic Republic of the Congo | 53. Republic of Guinea-Bissau |
| 18. Egypt | 54. Romania |
| 19. Eritrea | 55. Russia |
| 20. Estonia | 56. Saba |
| 21. France | 57. Saint Barthelemy |
| 22. French Guyana | 58. Saint Martin |
| 23. Germany | 59. Saint Pierre and Miquelon |
| 24. Greece | 60. Singapore |
| 25. Greenland | 61. Sint Maarten |
| 26. Guadeloupe | 62. Spain |
| 27. Guam | 63. South Africa |
| 28. Holy See (Vatican City) | 64. Somalia |
| 29. Italy | 65. South Sudan |
| 30. Iran (human rights) | 66. St. Eustatius |
| 31. Iran (nuclear proliferation) | 67. Sudan |
| 32. Iraq | 68. Syria |
| 33. ISIL and Al-Qaida | 69. Tunisia |
| 34. Ivory Coast | 70. Turkey |
| 35. Lebanon | 71. Ukraine |
| 36. Libya | 72. United Kingdom |

73.	USA	76.	Venezuela
74.	US Minor Outlying Islands	77.	Yemen
75.	US Virgin Islands	78.	Zimbabwe

The following categories of players will not be accepted at registration/post registration checks:

- Players under the age of 18.
- Players residing in non-reputable or banned jurisdictions,
- IP login registered in a non-reputable or banned jurisdiction,
- Sanctioned individuals,

However, on a case-by-case basis, the Company has the right to refuse any applicant for business or terminate an existing business relationship if the required Customer Due Diligence requirements are not satisfied. A deviation from the above may be applicable, on a case-by-case basis, following the approval of Senior Management.

7.4 Accepted payment methods

Certain payment options must be treated as high risk factors, this includes cash and other payment methods that may not leave or disrupt the audit trail and allow the customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies. The Company will only make use of the following payment methods: Credit Card, Bank Transfer, Internet e-wallets (EcoPayz, Interac, EzeeWallet, MuchBetter), offered by licensed financial institutions and regulated by an EEA financial regulator, approved by relevant Country Gaming authorities, where applicable.

The Company will always keep track of transactions carried out using these payment methods and identify funds that are received or remitted by customers.

In all instances, pay out money prizes and funds returned to customers shall be paid to the customer's originating payment method. If this is not possible due to the nature of the payment method or in case of the account not being available any more to receive funds, payments will be transferred only to an EEA bank account in the customer's name, following completion of the customer's due diligence process.

In all cases of credit cards, payment processors or bank transfers the additional verification methods used are to request:

- copy of the used credit card, whereby the first six and the last four numbers are clearly visible as well as the name of the holder of the card;
- a copy of the bank statement showing the customer's name, bank account number and the bank logo.
- a screenshot of the customer's account with the payment platform, showing the email address registered as well as the customer's name.

7.5 No cash policy

The Company does not accept cash deposits nor will cash withdrawals be processed.

8 Customer Due Diligence

The Company has an obligation to undertake CDD measures when:

- When players engage in financial transactions equal to or above Naf. 4,000;
- carrying out occasional transactions above the monetary equivalent of NAF. 4,000;
- there is a suspicion of money laundering or terrorist financing; or
- the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

The Company's CDD procedures require prospective customers to create a full profile at the point of registration. Mandatory information required at registration stage includes:

- Full name;
- Date of birth;
- Permanent residential address;
- Gender;
- Unique and verified email address;
- Phone number;
- Unique nickname; and
- Password.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents. This request is sent to the customer's registered email address. If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation. The documents must be clear and legible.

When requesting such documentation, the customer must always be informed by the Company that the card number must be blanked out leaving only the first 6 and the last 4 digits visible together with the expiry date.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Documents issued by the government that lack a photograph can be used to confirm the customer's current address, provided the address is included on the document.

In order to verify the details on their account, the customer is required to send customer care a photocopy or scan of one document from each of the categories listed below:

Personal Identification - one photo ID from the following list:

- 1) Current Signed passport
- 2) Current photo-card Driver's License (Provisional or Full)
- 3) Current Full Driver's License (old style paper version)
- 4) Current EU National Identify Card
- 5) Other recognized identity card such as an Armed Forces Identity Card

Address Verification - one of the following:

- 1) Utility bill (within the last 3 months)
- 2) Extract of the civil registry of the place of residence
- 3) Current photo-card Driver's License (Provisional or Full)
- 4) Current Full Driver's License (old style paper version)
- 5) ID card with address + Passport or additional ID
- 6) Bank/Credit Union/Building Society/Credit Card statement or passbook (within last 3 months)
- 7) Council tax bill or payment book (within the last 3 months)
- 8) Recent mortgage statement (within the last 3 months)
- 9) Current local council rent card or tenancy agreement (private tenancy agreements are not acceptable)
- 10) Home Insurance certificate or policy
- 11) Motor Insurance certificate or policy
- 12) Electoral roll
- 13) Credit reference agency
- 14) Mobile bills are not accepted

Source of Payment Verification/Proof of Payment - one of the following:

- 1) Copy of Credit or Debit card account statement of a card registered in name of the player (less than 3 months old)
- 2) Copy of bank statement - (less than 3 months old)

If a document submitted by a potential customer does not meet the verification standards, the compliance officer or designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay. If the customer cannot provide compliant documents within 30 days from the moment the Naf. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and report the transaction to the FIU.

All actions taken in response to non-compliant documents must be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

At this stage all customers will be screened through the automated/verification tools including the Sanctions- and PEP lists and adverse media through the company Namescan.io. Sanctioned customers cannot be accepted as customers. This shall be immediately escalated to the COMPLIANCE OFFICER and reported to the relevant authorities, as outlined in this Policy.

8.1 Simplified due diligence (SDD)

In low-risk scenarios, where the risks of ML/TF/PF are lower, simplified due diligence measures may be applicable, balancing the need for compliance with operational efficiency. Such measures include but are not limited to:

- Not collecting specific information: If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity.
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is upon the Company, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

At registration, customers have to fill in the following personal details:

- Full Name, (first and last name);
- Date of birth;
- Full Address (Street, City and Area);
- Country of residence;
- Gender;
- Email address;
- Phone number;
- Number and form of identification document; and
- They will also be required to create a username and password.

It is company policy not to allow players to deposit or withdraw any funds whatsoever before the registration process is complete.

8.1.1 Enhanced due diligence

Enhanced Due Diligence (EDD) will be implemented for customers identified as higher risk, consistent with the risks identified. In particular, the Company should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence must be conducted where the risks of money laundering or terrorist financing are higher. In any case, the following scenarios are subject to EDD:

- Residents of higher risk geographic areas;
- Political Exposed Persons (PEP's);
- Products or transactions that might favour anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. The Company will increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of EDD measures include but are not limited to:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

8.1.2 Politically Exposed Persons (PEPs)

A PEP is an individual who is entrusted with prominent public functions, other than middle ranking or more junior officials, including the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers,
- members of parliament or of similar legislative bodies,
- members of the governing bodies of political parties,
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- members of courts of auditors or of the boards of central banks,
- ambassadors, chargés d'affaires and high-ranking officers in armed forces,
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organisation.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

To identify if a client should be regarded as PEP the Company uses a variety of methods containing sufficient resources. The Company, on an ongoing basis, verifies whether its customers may be considered as PEPs by utilizing open sources and public databases. Should a

player who had not been identified as a PEP at on-boarding stage result to have become one, the casino is required to implement the measures described below within 30 days or terminate the relationship. The requirements for the EDD of PEPs shall apply also to relatives and close associates of PEPs, as defined in this Policy.

With respect to customers that have been confirmed as foreign PEPs, the Company shall:

- a. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- b. obtain senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction). Senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations. The approval can also be given from the manager of the Compliance department;
- c. take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The casino requests a statement from the player about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the information received, the casino can request the customer to provide documents; and
- d. conduct enhanced ongoing monitoring of the business relationship.

The Company shall take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, casinos are required to apply the measures referred to in items b, c and d. In accordance with the risk-based approach that the Company employs measures are tailored to the risk of the PEP, where the following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with the Company's legal obligations. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- The Company shall perform ongoing sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered and confirmed, the Company must follow the established Process for the freezing of resources as per the Sanctions Ordinance, and must immediately file a report with the FIU.

9 ONGOING MONITORING

Once a business relationship has been established, the National Ordinance for Identification when rendering services (NOIS) and the National Ordinance Reporting Unusual Transactions (NORUT) require the Company to carry out ongoing monitoring.

It incorporates two key elements:

9.1 Scrutiny and monitoring of transactions:

The Company shall monitor the transactions throughout the course of that relationship to ensure that they are consistent and in line with the customer behavior and his risk profile.

The transactions are monitored by an automated in-house monitoring system where Identity mismatches will be flagged for immediate manual review.

Where participants are flagged with a notification after the account opening, accounts are locked until customer due diligence procedures are in place. Some of the possible notifications that can be triggered are:

- SIPs, Watchlist
- A client residing or located in a country, the AML/CTF credentials about which the Company has doubts;
- A client who has been the subject of a disclosure
- A client flagged on the sanctions list.
- A client depositing gambling/withdrawing big amounts.
- A client flagged as a fraudster

To minimize the risks, all payments and fraud agents are instructed to consider instances where a customer uses a card belonging to a third party (i.e. the card holder's name does not match the customer's registered details). The account is blocked, explanation and documents requested from the client.

B) New or updated information and the documents of the clients:

During the periodic review of a customer, the Company verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (bad press/adverse news, incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behaviour of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

The Company requests fresh identification documents when the expiry date of identification documents held on file is reached. This can be done on a risk-sensitive basis or be linked to specific trigger events. Below is a non-exhaustive list of trigger events initiating a player review:

- High deposits/withdrawals;
- Suspicious gameplay activity;
- Non-wagering of funds;
- Mismatch in data (indicated data and/or digital fingerprint data);
- Mismatch in full name and credit card name
- Potential 3rd party usage;
- Registrations from the same IP;
- Usage of blocked credit cards;
- Potential minor usage;
- Links to other customers.

- Possible hits on screening of Sanctions and PEP-lists

The periodical review of the customer is based on the risk profile of the customer:

- For high-risk customers – once per year;
- For medium risk customers – once every 2 years;
- For low-risk customers – once every 3 years.

9.2 Fraud management

If the company cannot fulfil the player due diligence requirements, it must either not establish the business relationship or terminate it. The company must document all efforts to obtain the necessary information and documentation. Consequently, the company may choose to close the account or keep it fully blocked and suspended. If the player provides the required information or documentation after the account has been closed or suspended, the company must assess whether the delay impacts the risk of money laundering or terrorist financing associated with the business relationship.

The company should evaluate if there are any reasons to suspect money laundering, terrorist financing, or fraud. A player's reluctance to provide due diligence information should not automatically be seen as suspicious. The company should consider all available factors and information to determine if there are grounds for suspicion. If there is a presumption of money laundering, terrorist financing, or fraud, the company should report the unusual transaction to the FIU.

If there is no reason to retain the funds, they should be returned to the player through the same channels used to receive them.

If at any point that the customer does not comply with the Company's terms and conditions the Company may take the following actions:

- Request additional KYC documentation in accordance with the due diligence process described above
- Freeze funds in the account
- Cancel winnings and refund the deposits to the account
- Close the account
- Blacklist the players IP, device and/or payment account
- Reporting to the FIU and other relevant AML authorities by the COMPLIANCE OFFICER

10 REPORTING PROCEDURES AND OBLIGATIONS

All employees who engage with customers or have access to customer information receive anti-money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviors that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an internal report to the Compliance Officer (CO) in accordance with the Reporting Procedure. This ensures that the employee's legal obligation to report is fulfilled.

The following transactions or intended transactions are deemed unusual:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. 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);
- c. 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:
 1. A cashless transaction in the amount of NAf. 5,000 or more.
 2. Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the customer;
 3. 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.
 4. A cash out in the amount of NAf. 5,000 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

The Company is registered with FIU and has access to the goAML reporting portal.

10.1 Internal Reporting Procedures

By employing the procedures as described in this policy and the Anti-Fraud and AML/CTF System (the System) fully investigating any transaction, we can identify suspicious transactions or activities that could be construed as money laundering or terrorist financing. The system used is an in-house built anti-fraud monitoring tool.

Employees are required to report any unusual activity to the Compliance Officer immediately using an internal reporting form in writing using the standard template. The report must also include details on the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion. These reports must be made by the Company's employees when they have a suspicion in relation to a customer's behavior or when they receive an alert from the System. In the latter case, before submitting a report to the department responsible, the employee must check whether the alert is simply a false positive. The Compliance Officer will conduct a preliminary review of the reported activity within 24 hours to assess whether it requires further investigation. If a more in-depth investigation is necessary, the Compliance Officer will complete this within five (5) business days. During this time, the Compliance Officer may request additional information from relevant departments.

If the Compliance Officer concludes that the activity is unusual, an initial report must be submitted to the Financial Intelligence Unit Curaçao regarding any unusual or unusual monetary operations or transactions.

10.2 External reporting procedures

After considering the internal report and all the necessary documentation, when COMPLIANCE OFFICER determines that there is:

- (a) knowledge;
- (b) suspicion; or
- (c) reasonable grounds to suspect that:
 - a transaction may be related to ML/TF (regardless of the amount involved); or
 - a person may have been, is or may be connected with ML/TF; or
 - ML/TF has been, is being or may be committed or attempted;
- (d) Transaction amounts surpassing the respective thresholds as indicated per the objective indicators

The COMPLIANCE OFFICER shall file a UTR to FIU Curaçao and determines if reporting should also be done to other local authorities.¹

The COMPLIANCE OFFICER will not disclose the name of the employee who made the internal report to the FIU, and in completing this report COMPLIANCE OFFICER must provide as much detail as possible together with the relevant identification and other supporting documentation. The decision to file or not to file an unusual transaction report will always be at the discretion of the COMPLIANCE OFFICER, and COMPLIANCE OFFICER will not be subject to the direction or approval of other parties within the organization, provided that in reaching the decision on whether to file a report, COMPLIANCE OFFICER may seek assistance from other employees of the Company or external advisors.

An unusual transaction report form is available as ANNEX 1 to this document.

10.3 Prohibition of Disclosure

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to disciplinary action.

The Company has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the Financial Intelligence Unit Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions

¹e.g. Central Bank of Curacao and Sint Maarten

11 RECORD KEEPING PROCEDURES

In order to ensure compliance with the, the National Ordinance for Identification when rendering services (NOIS) and the National Ordinance Reporting Unusual Transactions (NORUT), as well as Implementing Procedures the Company ensures that the following records are maintained:

- 1) Record of CRA which is to include the following:
 - (i) a copy of each CRA carried out by the Company.
- 2) Records of CDD information and documents;
- 3) Record of business relationship with the details of transactions;
- 4) Record of internal reports to the Company;
- 5) Record of any determinations made by the Company and the designated employee, where applicable;
- 6) Record of STRs;
- 7) Record of AML/CTF training;
- 8) Record of conduct certificates or other documentation obtained in carrying out employee screening; and
- 9) Record of any outsourcing agreements.

In accordance with the local legislation the Company maintains all corporate records for a period of 10 years. The period for maintaining records related to AML/CTF and KYC documents is 5 years or longer when this extension is considered necessary for the purposes of the prevention of ML/TF. The time period commences from the date on which the business relationship is terminated, or the occasional transaction carried out.

The Company maintains these records in electronic form and in its physical files. Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Electronic records shall be stored in secure, encrypted databases with access controls to prevent unauthorized access. Physical records shall be stored in locked, fireproof cabinets within secure areas of the office. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure. Electronic records must be permanently deleted using secure deletion software that ensures data cannot be recovered. Physical records must be shredded using cross-cut shredders or incinerated to ensure complete destruction.

12 AML COMPLIANCE PROGRAM

12.1 Compliance Officer

A senior compliance officer will be designated, responsible for overseeing the AML program and ensuring compliance with regulations.

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

12.2 Employees

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing the Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

The employee due diligence process is informed by the Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate money laundering or terrorism financing must undergo screening. This requirement applies to:

- Prospective employees prior to their hiring for such roles.
- Current employees before they are transferred or promoted to such positions.

To screen both current and potential employees, the Company should:

- Identify the individuals.
- Verify their identity.
- Confirm their employment history, such as through references.
- Determine their suitability for the position and assess whether they pose any risk to the Company.

The Company will consider the knowledge and qualifications required for the responsibilities and authorities associated with each role.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether the employee:

- Has a criminal record, which may be verified through a police check.
- Is or has been subject to regulatory, court, or legal actions.
- Has leveraged bankruptcy laws for personal gain.
- Has resided in high-risk countries or regions.

Regular updates and re-evaluations are essential for maintaining an effective compliance program against money laundering, terrorism financing, and proliferation financing. This process includes conducting periodic reviews of all employees, with a particular emphasis on those in high-risk roles, to ensure their risk profiles are accurate and current. Additionally, reviews triggered by significant changes in an employee's job responsibilities, promotions, or external alerts that may influence their risk status are also initiated.

12.3 Training

In delivering AML/CTF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML/CTF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

The Company will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

The Company will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML/CTF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML/CTF that apply to the Company's staff.
- The launch of new products or services that alter the AML/CTF risk exposure.
- Instances where an employee breaches internal or external AML/CTF regulations due to a lack of knowledge during the performance of their duties.

The training shall be relevant to the respective employees' specific responsibilities and function within the Company. Through the training the Company shall ensure that the relevant employees are aware of:

1. CDD measures
2. Record keeping procedures
3. Internal and external reporting procedures
4. Customer Acceptance Policy
5. CRA policy

6. Relevant local and international legislation related to AML/CTF matters

The COMPLIANCE OFFICER shall be responsible for maintaining the Company's AML training materials. All the relevant employees shall undergo AML training upon commencement of their work and then have regular refreshers at least once a year.

12.4 Independent Audit Function

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML/CTF/CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate the Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

12.5 Examination by the Gaming Control Board

The Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the GCB during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

13 REGULARITY OF POLICY UPDATES

The Company must constantly monitor changes in legislation, FATF requirements and the general procedure for combating money laundering and terrorist financing.

The Company updates its internal anti-money laundering and anti-terrorist financing documents on an ongoing basis, but no later than three months after the entry into force of amendments to anti-money laundering and anti-terrorist financing legislation and / or identifying events that may to impact on AML-CTF POLICY.

APPENDIX 1

UNUSUAL TRANSACTION REPORT FORM

INTERNAL SUSPICIOUS ACTIVITY REPORT		
1. Date of report:		
2. Client name, Client ID and risk rating:		
3. Account status and account balance:		
4. Length of relationship/registration date of account:		
5. Client details (email, phone number, brand registration):		
a. Date of birth:		
b. Nationality/Country of registration:		
c. Address:		
d. Due diligence documents held:		
6. Crime/reason for suspicion (explain what activity or transaction gave rise to the suspicion i.e. the basis for suspicion) – if necessary, please use the additional information section:		
7. Date of suspected criminal activity/transaction:		
8. Provide details (e.g. dates and amounts) of any known transactions that are pending or due to occur in the future, if known:		
Name person making the report	Signature:	Date:

Upon completion, please forward the form to the department responsible as soon as possible.

9. Action taken by the responsible department		
Confirmation of the COMPLIANCE OFFICER: I confirm that I have received this UTR from the person/s named above.	Signature:	Date:

ADDITIONAL INFORMATION RELEVANT TO THE REPORT

(this should be used for anything that you think may assist the COMPLIANCE OFFICER, e.g. background on the suspect, details on the activity of the related account, further explanation of the transaction, IP addresses, excel sheet of all deposits and withdrawals, methods of deposits/withdrawals. If/where applicable that third party intelligence databases were used in the search, these need to be included.

NB: this page should not be attached where no additional information is provided)