

Anti-Money Laundering Policy
Cartwheel B.V

Version Control:

Version	Date	Description of change	Author
1.0	08.04.2024	Creation of Policy	Compliance Officer
1.1	16.04.2024	Legal framework amended to align with relevant regulation. Addition of sections to align with updated regulations.	Director
2.0	03.04.2025	Policy over hall and updates made according to newly enforced regulation	Compliance Officer

Table of Contents

DEFINITIONS AND ABBREVIATIONS	5
INTRODUCTION	7
UNDERSTANDING MONEY LAUNDERING AND FUNDING OF TERRORISM	8
WHAT IS MONEY LAUNDERING AND TERRORIST FINANCING?	8
<i>Money Laundering</i>	8
<i>Terrorist Financing</i>	8
<i>Financing the proliferation of weapons</i>	8
SCOPE.....	9
LEGAL FRAMEWORK	10
INTERNATIONAL REGULATIONS	11
THE ROLE OF THE COMPLIANCE OFFICER	11
COMPLIANCE OFFICER DETAILS	12
THE FUNCTION OF THE RISK BASED APPROACH (RBA) AND RISK MITIGATION	12
ONBOARDING OF NEW AND PROSPECTIVE CUSTOMERS	13
NEW REGISTRATION CHECKS	14
RISK APPETITE AND CUSTOMER ACCEPTANCE	14
BUSINESS RISK ASSESSMENT	14
THE COMPANY CONDUCTS A BUSINESS RISK ASSESSMENT (BRA) TO EVALUATE INHERENT RISKS, THREATS, AND VULNERABILITIES, USING A RISK-BASED APPROACH TO DETERMINE THE RESIDUAL RISK AFTER MITIGATION. THE BRA INFLUENCES THE COMPANY'S POLICIES, INTERNAL CONTROLS, AND COMPLIANCE PROCEDURES, WHICH ALL EMPLOYEES ARE REGULARLY TRAINED ON.....	14
CUSTOMER RISK ASSESSMENT.....	15
PURPOSE AND NATURE OF THE RELATIONSHIP	15
CUSTOMER DUE DILIGENCE.....	16
TIMING OF DUE DILIGENCE MEASURES.....	16
LEVEL 1: CUSTOMER DUE DILIGENCE (CDD)	16
<i>Identification Verification</i>	17
<i>Address verification</i>	17
LEVEL 2: CUSTOMER DUE DILIGENCE (CDD)	18
LEVEL 3: CUSTOMER DUE DILIGENCE (CDD)	18

Information on the economic profile	19
LEVEL 4: ENHANCED DUE DILIGENCE (EDD)	19
SOURCE OF FUNDS AND WEALTH	20
CUSTOMERS FAILING TO PROVIDE DUE DILIGENCE INFORMATION	21
ONGOING AND TRANSACTION MONITORING	21
PERIODIC ONGOING MONITORING AND REVIEW FREQUENCY	22
TRANSACTION MONITORING	22
CUSTOMER SCREENING	23
POLITICALLY EXPOSED PERSONS (PEPS)	23
<i>Client Risk Classification</i>	24
THE MONITORING OF ACCOUNT HOLDER ACTIVITIES	24
<i>Unusual activities</i>	25
<i>Deposits and Withdrawals</i>	25
<i>Transactions using Cryptocurrency</i>	26
REPORTING PROCEDURES (RP)	26
SUSPICIOUS ACTIVITY OR TRANSACTION	26
RECOGNITION OF UNUSUAL TRANSACTIONS	26
DOCUMENTATION OF UNUSUAL TRANSACTIONS	27
REPORTING OF UNUSUAL TRANSACTIONS	27
Internal Reporting	27
Reporting Criteria	28
TIPPING-OFF AND PREJUDICING AN INVESTIGATION	28
TIPPING- OFF	28
PREJUDICING AN INVESTIGATION:	29
PUNISHMENTS FOR TIPPING-OFF AND PREJUDICING AN INVESTIGATION:	29
EXCEPTIONS:	29
EMPLOYEE SCREENING	29
KNOW YOUR EMPLOYEE	29
EMPLOYEES TRAINING	30
Periodicity	30
Scope	30
TRAINING RECORDS	31
INTERNAL AUDITING	31

Definitions and Abbreviations

Account Holder	An individual who has a Player Account on the Website.
Anti Money Laundering ("AML")	All efforts focused on the prevention of money laundering, the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.
Caribbean Financial Action Task Force ("CFATF")	An organization of states and territories of the Caribbean territory that have agreed to implement common countermeasures against money laundering and terrorism financing. (www.cfatf-gafic.org)
Combatting terrorist financing ("CFT")	All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
Combatting proliferation of weapons of mass destruction ("CPWMD")	Efforts aimed at combatting the financing or provision of funds for the sale, transfer, or export of nuclear, chemical or biological weapons, their delivery systems and related materials.
Cryptocurrency	Distributed, open-source, mathematically based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include Bitcoin, Ethereum, Litecoin and Dogecoin.
Cryptocurrency transaction	The deposit and withdraw of cryptocurrencies into and out of a Player Account held by a Player.
the Company	[CLIENT COMPANY NAME] N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number [number].
Employee	Any person working for the Company.
Financial Action Task Force ("FATF")	An intergovernmental organization dedicated to developing standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. (www.fatf-gafi.org)

Financial Intelligence Unit (“FIU”)	Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of suspicious transaction reports (STR) and other information regarding potential money laundering or terrorist financing.
Know Your Client (“KYC”)	Know Your Client, the mandatory process of identifying and verifying the client's identity when opening a Player Account and periodically over time.
Money Laundering (“ML”)	A process through which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise, or attempt to disguise, such proceeds to make them appear to be legitimate.
Money Laundering Reporting Officer (“MLRO”)	Designated individual in charge of the review of KYC information and the monitoring of Player Account activities. The MLRO might further be assisted by designated personnel.
Player	Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened providing him/her with a unique code.
Player Account	An account granted to an individual after registration on the Website. The Player 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 IP address, per family and per Shared Environment.
Politically Exposed Person (“PEP”)	A person entrusted with a prominent public function, such as a senior political figure. Individuals closely related to this person, for instance immediate family members and close associates, are also considered PEPs. PEPs are classified as a Money Laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.
Prohibited Jurisdictions	Jurisdictions prohibited under the Curaçao license conditions by the Curaçao Gaming Authority at a certain moment, jurisdictions restricted by decision of the Company's managing director at a certain moment when and where still applicable, as well as countries mentioned on the FATF blacklist or on which any financial sanctions has been imposed by the EU/ U.N. and/or the OFAC.

Proliferation Financing (“PF”)	The act of providing funds or financial services which are used, in whole or in part, 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 (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
the Regulator	The Curaçao Gaming Authority (CGA). The regulator for the entire gaming industry operating in and from Curaçao.
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 offices. Only one Player Account is permitted per Shared Environment.
Service	the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.
Terms and Conditions	The terms and conditions for the use of the Services, as published on the Website.
Terrorism Financing (“TF”)	The process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities.
Website	the online gaming platform offering online gaming services operated by the Company.

Introduction

Cartwheel B.V. also referred to as (the “Company”) is a Curacao Limited company, established to offer remote gaming services, specifically Casino.

Understanding Money Laundering and Funding of Terrorism

What is money laundering and terrorist financing?

Money Laundering

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. There are three stages in the process:

Placement: The placement stage is when money enters the financial system. At this point, it's still possible to trace the funds back to their illegal source. This stage kicks off the money laundering process, aiming to integrate illicit funds into the financial system. During this stage, it's crucial for the company to understand where its customers' funds come from, as criminals trying to launder money will want to get rid of it without drawing attention.

Layering: Layering is used to convert the proceeds of the crime into another form by creating complex layers of financial transactions to obfuscate the source and ownership of funds. This process is directed at trying to confuse any investigation by making it difficult to trace the origin of the funds. For example, this could involve electronically moving funds from one jurisdiction to another, moving funds between different financial institutions or to different accounts within the same financial institution.

Integration: At this stage the money derived from criminal activity has been made to appear legitimate and is placed once again into the financial system in what appears to be normal business or personal transactions. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth.

As it is strictly a Company policy not to accept cash as means of payment, the Company's AML Policy is focused to prevent the use of the Company's activities and resources in the 2nd and in the 3rd stage.

Terrorist Financing

“**Terrorist financing**” means financing acts of terrorism. Terrorist financing is a very serious threat to financial services and businesses and must be taken as seriously as money laundering.

When dealing with terrorist financing, it is important to note that funds do not necessarily have to be derived from criminal activities. The funding of terrorism can adopt a similar methodology to that used for money laundering however the intent and the scope of such acts vary from one another. The Professional Standards enforce Customer Due Diligence and KYC on transactions and have made the activity of terrorist financing more difficult for those who are willing to pursue it.

Financing the proliferation of weapons

The Financing of Proliferation of Weapons refers to the financial support of activities that help develop or spread nuclear, chemical, or biological weapons. This includes illegal financial transactions that support the creation, acquisition, or distribution of such weapons.

Money Laundering, Terrorism Financing and proliferation of weapons of mass destruction are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Individuals involved in ML and/or TF continually attempt to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such individuals

must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

ML in the online gaming industry manifests itself in two opposing forms:

- a) the use of criminal funds to fund gambling activities; and
- b) the exchange of criminally acquired funds for legitimate money.

In both cases, authorities fear that those phenomena damage sports, the online gaming industry, and society as a whole. Therefore ML, when not eliminated, can have far-reaching implications.

TF may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for unlawful purposes. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures. PFWMD may involve the sale, transfer, export, of weapons of Mass destruction, like nuclear weapons and atomic weapons. Such proliferation must be countered as well due to it posing a signification threat to international peace and security, as identity by relevant United Nations Security Council Resolutions (UNSCRs). Therefore, the CP measures involve identifying and assessing the risks of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. The Company's procedures and internal controls are designed to ensure compliance with all applicable national and international regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

To accomplish this task, the Company uses policy development, various controls, procedures and training to not only provide a clear understanding of anti-money laundering concepts, legal obligations, relevant offences and practical safeguards, but also to reinforce these through a strong culture of ethics and compliance.

Scope

The scope of this policy is to establish policies and procedures on internal controls, risk assessment, risk management and compliance in relation to AML, CTF and CPF.

The policy has been created in compliance with the licence held within the Curacao jurisdiction and ensures to:

- Remain alert to the possibility of ML, TF or PF
- Report all suspicions to the Compliance Officer email address in accordance with the AML/CTF policy.
- Comply fully with all AML procedures including: customer identification, monitoring, record keeping, awareness and reporting in accordance with their respective roles and responsibilities within the company;

- Attend any relevant training and keeping up to date with new and evolving threats;
- Complete the mandatory AML/CFT Training periodically to ensure compliance and adherence to the policy;
- Ensure that the company is not used for illicit activity and does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with ML, TF and PF;;
- Take the most reasonable and appropriate actions to mitigate the risks associated with ML, FT, PF and other financial criminal activities, including fraud, corruption etc.
- terminate any relationships where the Account Holder's conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations;

This policy and procedure is applicable to all employees, contractors, affiliates and any other individual working on behalf of the Company. The Company is determined and committed to prevent the carrying out of financial activities through its systems that may be related to ML or FT. This Policy defines procedures that will assist all persons working for the Company to comply with its legal obligations.

The Company shall comply with its obligations at law by establishing the necessary and relevant processes to prevent ML and FT and to ensure any suspicious activities are escalated to the relevant authorities. The policies outline the general and minimum standards of internal AML, CFT and CPF which should be adhered to by the companies management and employees.

Legal Framework

Pursuant to the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao.

Further main national regulations relating to money laundering and terrorist financing are the following:

- a) The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G.2024, no.41(N.G.2017, no.92)(NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2024 no.41 (N.G. 2017, no. 99)) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- e) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93); and

- f) National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.
- g) National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- h) Kingdom Sanction Act (N.G. 2016, no. 54);

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

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 an international level, the FATF plays an important role in the combating of ML, TF and PF. The FATF monitors the progress of its members in implementing necessary measures, reviews ML and TF techniques and countermeasures, 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.

Subsequently the present policy is a combination of the FATF 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.

The Role of the Compliance Officer

The Company has designated a senior management-level Compliance Officer, independent from the gaming operations, responsible for ensuring the detection and deterrence of money laundering and terrorist financing. The Compliance Officer is entrusted with the following duties:

- **AML Program Design and Implementation:** Develop and enforce the AML program to comply with local laws and regulations.
- **Policy and Procedure Review:** Ensure adherence to the Company's internal AML policies and procedures.
- **Staff Training:** Organize and deliver ongoing compliance training for staff.
- **Transaction Monitoring:** Analyze and assess transactions for potential suspicious activity, ensuring compliance with the Ministerial Decree on Indicators for Unusual Transactions.
- **Reporting:** Review, maintain records of, and report internally and externally any unusual transactions.

- **Investigation and Reporting:** Conduct investigations into unusual transactions when necessary and prepare external reports as required.
- **Account Freezing:** Develop internal procedures for blocking or freezing user accounts, taking care to avoid tipping off the player.
- **Program Improvements:** Remain informed on AML/CFT developments and propose necessary changes to the AML program.
- **Periodic Reporting:** Prepare and submit periodic reports on the Company's AML/CFT efforts.

The Compliance Officer is granted access to customer identification data, transaction records, and other relevant information and has the authority to act independently in carrying out these duties. The Compliance Officer's job description, including these responsibilities, is signed and dated to confirm acceptance of the role.

Compliance Officer Details

The company has appointed the following Compliance Officer

Name: Sabina Ramadan

Email: compliance@cartwheelglobal.com

The Function of the Risk Based Approach (RBA) and Risk Mitigation

Considering the assessed risks from the CRA, the Company shall determine the type and extent of measures it will adopt to manage and mitigate the identified risks in a cost-effective manner. The RBA adopted by the Company is devised in a manner that reads multiple factors in order to determine an adequate score. Customers who are natural persons shall follow an automated risk assessment and those who present a higher than average risk or where a customer's transactions fall under large or complex conditions shall automatically alert the compliance department for a manual review.

The automated risk assessment shall be, based on a set of criteria established within the product and the jurisdictional risk assessment, established periodically by the Compliance Officer. The manual risk assessment shall be able to establish:

- The customer's Due Diligence level in line with their assessed ML and FT risk;
- The areas of risk that the customer is likely to pose;
- Implement a level of due diligence and risk-based controls that manages and mitigates the risks;
- Obtaining additional data and information from the customers, where this is appropriate for the proper and complete understanding of their activities and source of wealth;
- Requiring the quality and extent of identification data for each type of customer to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence, certification and verification of documents);
- Determine if the customer falls within the Company's risk appetite; and
- monitoring and improving the effective operation of these controls and identifying any weaknesses;
- and recording what has been done and why.

The list is NOT exhaustive, and officers can request any documentation deemed necessary to address any threat the customer may pose. The risk assessment shall reflect reasonable rationale and justification for the risk level assigned.

The Compliance Officer will develop and constantly monitor and adjust the Company's policies and procedures concerning the customer Acceptance Policy and customer Due Diligence and Identification Procedures, respectively. The Compliance Officer will also monitor the process via a random sampling exercise. These actions shall be duly documented in board resolutions as determined by the chairman of the Company.

Onboarding of New and Prospective Customers

This section describes the criteria for accepting new customers based on their risk categorisation. Following a risk-based approach for every customer, it will be determined what level of due diligence is to be applied concerning identification, business relationship and transaction level. Where the level of risk is above the level the Company is willing to accept, appropriate steps must be taken to mitigate the risk. If the risk cannot be mitigated to an acceptable level, the relationship must be terminated.

The customer on account registration, shall provide the following identification information:

- First name
- Last name
- Date of birth
- Residence address (Building, street, city, country)
- Email and/or mobile phone number

The Company interfaces with customers non-face to face due to this the Company has implemented mandatory verification for which tools and technology will be utilised to limit the risk from non-face to face. The Company shall reserve the right to block accounts and request alternative documentation should it be deemed necessary.

In order for the Company to know it is dealing with a real person, documentation is required to corroborate as much as the information submitted as possible, the Company shall obtain sufficient evidence of identity to verify the person is whom they claim to be.

A customer's residential address is an essential part of their identity, and when it is not present on identification documents, it will have to be obtained separately (once the relevant due diligence level is reached).

The KYC provided will be verified manually to ensure that the documentation provided corresponds to the information currently held on the customer and that the KYC is valid. If the documentation provided is deemed not to be valid or sufficient, further documentation may be requested from the customer.

Following the risk-based approach, at onboarding, an automated risk assessment of the ML and FT risk posed by the customer is carried out based on the information provided by the customer and checks conducted. The risk assessment will rate the customer as low, medium or high risk, due diligence and ongoing monitoring will be carried out in proportion to this risk. If the risk is deemed Medium or High, further information and documentation is required from the customer. If the account is exhibiting trends or there is suspicion, knowledge or reason to believe it must be reviewed by compliance personnel and brought to the attention of the Compliance officer for approval and analysis.

New registration checks

Every customer can open only one account per brand/website. If a customer tries to open multiple accounts, these will be blocked.

In addition, the customer's IP address is registered upon every log-in. Upon registration, a review is done as to whether the customer's IP address corresponds to the registered country. If there is a mismatch, the customer account is flagged for further checks.

Risk appetite and Customer Acceptance

The Company currently has a high risk appetite when it comes to customer acceptance but a medium risk business appetite meaning that the residual risk of any product or service has to have sufficient controls in place to mitigate such risk to be within controllable boundaries and for which the Company has control over the behavioral pattern and relationship with the customer.

The policies and procedures hereunder are all reflective of such concepts and are therefore in place to further activate the desired result in ensuring proper risk management and mitigation. The risk categorization is defined in the Company's Customer Acceptance Policy (CAP).

Business Risk Assessment

The Company conducts a Business Risk Assessment (BRA) to evaluate inherent risks, threats, and vulnerabilities, using a risk-based approach to determine the residual risk after mitigation. The BRA influences the Company's policies, internal controls, and compliance procedures, which all employees are regularly trained on.

The BRA covers all services, customer transactions, and jurisdictions, using both qualitative and quantitative methods to assess risks related to customers, payment methods, and geographic locations. The results guide the determination of whether the risks fall within the Company's acceptable risk appetite.

If any identified risks exceed the acceptable level, additional mitigation measures will be implemented. The BRA considers factors such as:

- Customer
- Transaction
- Geography
- Source of Funds

Risks are categorized as low, medium, or high, and the BRA is reviewed annually, or sooner if there are changes to services, jurisdictions, or regulations, in line with Curaçao's AML requirements.

The Company also considers the outcomes and recommendations of the National Risk Assessment in the BRA, ensuring alignment with the latest regulatory requirements.

By following this risk-based approach, the Company continuously monitors developments in money laundering and terrorist financing and adjusts its measures to mitigate emerging risks.

Customer Risk Assessment

The Company uses a risk-based approach to anti-money laundering (AML) to ensure its systems and controls are tailored to the specific money laundering risks it faces. This approach moves away from a "one size fits all" model and allows the Company to identify and address risks based on customer behavior.

By understanding the risks posed by various factors, the Company has implemented strong risk management practices and tools to monitor and mitigate money laundering (ML), financing of terrorism (FT), and other illicit activities.

The level of due diligence required varies based on the customer's actions and behavior. The Company's approach to customer risk assessment (CRA) includes:

- Risk Assessment: Identifying customer behavior patterns and relevant risk factors.
- Transactional Triggers: Monitoring transactions that may indicate potential ML/FT risks, requiring internal analysis.
- Customers are assigned a risk score (Low, Medium, or High) based on factors such as:
 - Geographic risk
 - Customer risk
 - Interface risk
 - Product risk
 - Payment and transaction risk
 - Gaming behavior patterns

The customer's risk score is updated based on their behavior and transaction patterns. If necessary, alerts can be cleared after manual review or if the customer provides sufficient information. Any changes to the risk score are documented, and must be approved by the Compliance Officer, with written justification on the customer's account.

Purpose and Nature of the Relationship

In the remote gaming sector, the purpose behind opening a gaming account is clear – customers want to access gaming services. Based on this, it is not required to gather additional information solely for the purpose of account creation. However, understanding the customer's activities and purpose is essential for effective Customer Due Diligence (CDD) and risk assessment.

The Company must build and document the customer's economic profile, ensuring all relevant due diligence information is collected to verify the customer's identity. The AML/CFT team may also request additional documentation if needed to understand the source of funds and the nature of the transactions.

For customers making transactions, we will compare their actual activity with expected account turnover. Any significant deviations from usual activity will be investigated for potential money laundering (ML) or terrorist financing (FT) concerns. If necessary, an internal **Unusual Transaction Report (STR)** will be submitted to the Compliance Officer, and the findings will be documented in the customer's file.

All customers must have a business relationship with the Company, meaning the necessary due diligence will be completed for all customers. For customers making occasional transactions (transactions outside of an established business

relationship), the same due diligence will apply to activate the account. This business relationship will remain in place for up to 12 months in the case of inactivity before being terminated

Customer Due Diligence

In accordance with the Customer Due Diligence measures outlined under Article 7 of the Prevention of Money Laundering and Terrorist Financing Regulations of 2024, it is the policy of this Company to conduct a risk assessment and ensure that evidence of the customer's identity is obtained and retained as required for all clients.

Timing of Due Diligence Measures

In accordance with the Curaçao Gaming Control Board (GCB) regulations, Customer Due Diligence (CDD) measures are required in the following situations:

Establishing Business Relationships: Prior to initiating any business relationship with a customer, CDD measures must be applied.

Occasional Transactions: For transactions amounting to or exceeding the equivalent of XCG. 4,000 (approximately €2,000), whether conducted as a single transaction or a series of linked transactions, CDD measures are mandatory.

Suspicion of Money Laundering or Terrorist Financing: If there is any suspicion that a transaction involves funds linked to money laundering or terrorist financing, CDD measures must be undertaken.

Doubts About Previously Obtained Customer Information: When there are uncertainties regarding the veracity or adequacy of existing customer identification data, CDD measures should be revisited and updated as necessary.

LEVEL 1: Customer Due Diligence (CDD)

The Company CDD Level 1 requires customers to only be able to deposit to a maximum aggregate value of less than XCG. 4,000 (approximately €2,000), cumulatively lifetime or in one lump sum. Level 1 consists of the provision of the:

- Customer's Email and/or Mobile number;
- Basic customer information:
- Official full name
- Date of birth (to calculate age)
- Permanent residential address.
- ID card number
- Gender
- Username and a password

At Registration customers are classified in risk categories according to their risk profile - low, medium or high.

The Company has elected to carry out identification and verification of the customer's identity and address via documentation on the customer's first deposit and or withdrawal.

Upon the Company requesting CDD documentation, a 30-day time period will start for the provision of documentation, during which withdrawals will be suspended. Upon the lapse of the 30-day time period, and CDD documentation is not provided or not successfully completed, the customer's account will be suspended from deposits and wagers as well.

Identification Verification

The customer is subject to identity verification which shall be outsourced to a third party provider and if required also have the ID document screened against www.edisontd.nl if upon testing, suspicion is raised in relation to adequacy of the document. The term outsourced means will provide the technology but all obligations and responsibilities shall be kept within the Company. All customers entering the platform shall be subject to completion of identification including PEP, Financial Sanctions and Negative Media checks for which the following is to be obtained:

1. Identity verification;
2. Address Verification
3. A selfie.

Identity verification of the customer is to be provided as a form of government-issued document/s, such document/s should contain photographic evidence of identity. Acceptable documentation shall be as follows:

- a valid passport preferably does not expire in the following six (6) months;
- a valid national or other government-issued identity card;
- a valid residence card; or
- a valid driving licence (must hold nationality

For the provisions relating to identification procedures and CDD requirements, proof of identity is satisfactory if:

- It is reasonably possible to establish that the customer is the person he claims to be; and
- The person who examines the evidence is satisfied that the customer is actually the person he claims to be.

If there is a suspicion regarding an identification document further documentation is to be requested. Those customers who do not reside within the European Union and reside in a high-risk jurisdiction or where the customer presents a high ML/FT risk, the Company shall reserve the right to request further information and documentation pertaining to the customer in order to satisfy any risk or questions related to the identified threat.

An assessment of the provider's systems capabilities has been carried out, and the following criteria has been met:

- The ability of the software to assess the KYC received for validity and that the details provided match the customer's; and
- The retention of the documents uploaded shall be held in accordance with the record keeping section hereunder.

It is pertinent that the documents are held on file for a minimum of 5 years. All documents, including any correspondence or re-uploading of documentation, shall be kept on file. The time and date of actions and uploading of documents shall also be kept on file. The records may not be altered, tampered with or manipulated upon upload completion.

Address verification

At this stage (CDD), the customer's address shall also be verified. The address is verified by obtaining one of the following documents (which are not more than six months old) that clearly shows the customer's name and residential address:

- A recent utility bill preferably not older than six (6) months;
- A recent statement preferably not older than (6) months, from a recognised credit institution;
- Correspondence from a central or local government authority, department or agency;
- A record of visit to the address by a senior official of the subject person;

- Any identification document where a clear indication of residential address is provided; or
- Certificate of conduct issued by a law enforcement authority.

In relation to utility bills when verification of a utility bill is done by the Company it is to verify that the said document has been issued in relation to the services linked to that residential property. A bill issued in relation to a fixed line telephone service installed on that property would be also acceptable. Mobile telephone bills which are not linked to a fixed premise are not acceptable.

The address verification documents will be uploaded via the provider who will ensure:

- The documents provided are a valid form of Address Verification documentation (see the list of acceptable address verification documentation above);
- The documents provided are not more than 6-months old.
- The details provided on the address verification documentation match the customer's account.
- The address verification documentation looks legitimate and not tampered with; and
- The address verification documentation is held on file for a minimum of 5 years.

If there is a suspicion regarding the address verification document further documentation is to be requested.

Those customers who do not reside within the European Union but reside in a high-risk jurisdiction or where the customer presents a high ML/FT risk the Company shall reserve the right to request further information and documentation pertaining to the customer to satisfy any risk or questions related to the identified threat.

The Company understands that CDD is a dynamic ongoing process; throughout ongoing monitoring, certain changes, events or triggers will require the Company to re-complete some or all the CDD measures. The completion of CDD will result in a customer either successfully passing CDD or alternatively being classified as high risk and being immediately subject to EDD (level 4).

N.B. if a customer has a change in I.P. of over 90 days, the customer will be prompted to update the proof of address.

LEVEL 2: Customer Due Diligence (CDD)

The Company CDD Level 2 incorporates customers whose gross deposits reach XCG. 4,000 (approximately €2,000), cumulatively lifetime or in one lump sum, and the risk assessment is deemed as low risk. This stage includes the following:

- Identifying and verifying the customer's identity and address via documentation (if not already done at Level 1);
- Identifying the beneficial owner where this is not the customer;
- Conducting ongoing monitoring of the business relationship.

LEVEL 3: Customer Due Diligence (CDD)

The Company CDD Level 3 incorporates customers whose gross deposits reach XCG4,000 (approximately €2,000), cumulatively lifetime or in one lump sum, and the risk assessment is deemed as medium risk. This stage includes the following:

- Identifying and verifying the customer's identity and address via documentation with photograph (if not already done at Level 1 or 2);

- Collect additional personal details;
- Collect source of wealth information;
- Identifying the beneficial owner where this is not the customer;
- Obtaining details expected level of spending; and
- Conducting ongoing monitoring of the business relationship

Information on the economic profile

The following information is obtained at CDD level 3 to provide information on the economic profile of a customer. This information shall be used to further substantiate the business relation and provide the Company with relevant information pertaining to the source of wealth and funds used in the business relationship. This is detailed within the Customer Acceptance Policy (CAP).

A manual review of the account shall be conducted to ensure the customer is properly risk assessed and to corroborate as much of the source of wealth information provided as possible via open source intelligence. Research shall be carried out on those customers for which have raised concern in relation to the funding of the account or upon review. If there is a mismatch between the information provided by the customer and background research, this could lead to a ML/FT concern leading to the customer being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

LEVEL 4: Enhanced Due Diligence (EDD)

The Company CDD Level 4 incorporates customers whose gross deposits reach XCG. 4,000 (approximately €2,000), cumulatively lifetime or in one lump sum, and the risk assessment is deemed as high risk, such as if a customer is a PEP. This stage includes the following:

- Identifying and verifying the customer's identity and address via documentation with photograph;
- Collect additional personal details;
- Collect source of wealth information and documentation;
- Identifying the beneficial owner where this is not the customer;
- Obtaining details expected level of spending; and
- Conducting ongoing monitoring of the business relationship.
- verifying the disclosed details against certain (public or private) databases (e.g. sanction lists)

EDD is to be applied without delay in instances where the customer is likely to pose a higher than normal ML/FT risk. EDD shall require additional measures concerning where the threat is emanating from achieved via source of wealth/funds requests. The Company is to keep all documentation regarding the customer's identity, documentation verification and the risk assessment.

Once EDD has been completed the residual risk is to be adequately assessed in the risk assessment and sufficient ongoing monitoring is to be conducted to address any residual risk. If the residual risk is greater than the Company's risk appetite (and cannot be lowered to a satisfactory level by mitigating measures) the account shall be terminated.

EDD verification measures are as follows (note that each will not be required on every EDD verification but based on the information provided by the customer and the risks presented):

- Obtaining additional information and, as is appropriate, substantiating documentation on the intended nature of the business relationship;

- Carrying out additional searches (e.g., internet searches using independent and open sources) to better inform the customer's risk profile;
- Consider the source of wealth and funds involved in the transaction or business relationship to ensure they do not constitute the proceeds of crime. In order to investigate this it could include obtaining appropriate documentation concerning the source of wealth or funds even on the beneficiaries; See the 'Source of Funds and Wealth' sections below for more information regarding the SOW/F process;
- Increasing the frequency and intensity of transaction monitoring; Increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
- Increasing awareness of higher-risk customers and transactions across all departments who have a business relationship with the customer. Increasing awareness also includes the possibility conducting enhanced briefing with engagement teams responsible for the customer; and
- Obtain Senior Management approval for the continuation of the relationship in cases where the doubt has been raised on approval of the customer.

High-risk customers will be identified and placed on a High-Risk Customer Report generated in the Back Office. For these customers, the system will automatically trigger an alert every 12 months or whenever transactional triggers are activated. The Compliance Officer has the authority to override any risk assessment and place customers on this high-risk monitoring list, which will result in their relationship being assessed more frequently.

If a customer successfully passes EDD verification a threshold of 45% of the customer's verified income is added and ongoing monitoring will continue with the aim of identifying any possible suspicious transactions or activity which would need to be investigated further.

We can only request information from the customer which assists us in addressing a concern or understanding how the customer is financing their activity.

If a customer refuses to provide any information or fails to provide the necessary information within the relevant time period, we will suspend the account and stop processing any further wagering and shall be effectively blocked. The case shall be raised further with the Compliance officer assigned to decide whether the case warrants further reporting to the relevant authority by analysing activity to identify knowledge, suspicion or reason to believe ML/FT.

Source of Funds and Wealth

Source of Funds (SOF) refers to how the funds for a transaction are generated, while Source of Wealth (SOW) describes the activities contributing to a customer's total net worth. We are not required to investigate every customer's financial history, but we must ensure that transactions align with the customer's profile.

SOF/SOW may be requested based on the customer's risk profile or specific circumstances such as:

- Medium or High-Risk Customers following a risk assessment (CRA)
- Negative Media Hits related to fraud or financial crime
- Customers involved in trading financial assets
- High-risk jurisdictions or suspicious financing sources

If the source of funds is from high-risk or non-reputable jurisdictions, the customer should be flagged for review by the Compliance Officer. Other triggers include suspicious activity, inconsistent transactions with the customer's profile, or third-party funding.

We will request SOF/SOW documentation to understand how the customer funds their transactions. Documentation and evidence must be maintained and updated regularly. If concerns about the source of funds arise, we will consider submitting an Unusual Transaction Report (UTR) to the Compliance officer.

Examples of Documentation:

- **Salary:** Bank statements showing salary deposits, payslips, tax returns.
- **Company Profits:** Dividends certificate, company bank statements.
- **Sale of Property:** Contract of sale, bank statement showing proceeds.
- **Gift:** Letter from the donor, bank statement showing the gift.

All investigations into SOF/SOW must be documented, with clear justification for the level of due diligence applied. If concerns persist, further documentation or a UTR may be required.

Customers Failing to Provide Due Diligence Information

Where we are unable to apply Due Diligence measures, the general rules are that we must:

- Not carry out a transaction for the customer;
- Not accept funds from or transfer funds to a customer;
- Not establish a business relationship with a customer;
- Terminate any existing business relationship with the customer; and
- Consider whether an UTR is required.

There are very limited circumstances in which the above rules will not apply, e.g. we may not be able to verify the customer's identity during establishing a business relationship. This action may be necessary to avoid interrupting the normal course of business and where there is little risk of ML. This action is only allowed on the condition that the verification is completed as soon as practicable after first contact is established. The decision to delay Due Diligence measures must never be unilaterally decided and a note should be left with the rationale of such action.

Customers shall be given a 30-day timeframe from the date of first correspondence to respond to due diligence information requests. The customer will be allowed to deposit and wager only. No withdrawals will be allowed. These 30 day time periods shall be extended depending on the correspondence and information provided by the customer. If the customer does not provide the Due Diligence information required within 30 days from the last day of correspondence, the account shall be blocked in its entirety, and the user when accessing their account will only be able to see the information request which will need to be answered in order to unblock the account.

In relation to EDD (SOF/W) information requests, if the customer does not respond to the request they will be sent reminders on day 7, 15 and 25 from the date of the first correspondence. If the customer does not provide within 30 days the account will be blocked accordingly.

Ongoing and Transaction Monitoring

Ongoing monitoring is essential for detecting unusual or suspicious transactions, regardless of the customer's risk rating. All transactions are monitored to ensure they match what the Company expects based on the customer's profile and behavior.

The Company tracks transactions for signs of:

- Deviations from expected patterns based on customer due diligence (CDD).
- Unusual behavior that might suggest illegal activity.
- Potential links to money laundering (ML) or terrorist financing (FT).

Key risk factors to watch include:

- Gambling or transaction patterns that differ from the customer's usual activity.
- Unusually large transactions.
- Requests to withdraw funds to an unverified account (which is not allowed).
- Requests to transfer funds or winnings to another person (which is also not allowed).

The goals of ongoing monitoring are to:

- Ensure transactions align with the customer's known profile and legitimate sources of funds.
- Keep customer documents up to date and flagged for expiration.
- Monitor for changes in the customer's risk profile.
- Look for possible signs of ML/FT in transactions.

The Company will investigate transactions that are complex, large, unusual, or have no clear lawful purpose. If any transaction raises suspicion, the customer's risk profile may be upgraded to High, and additional documentation may be requested.

If discrepancies or suspicious activities are noted, a manual review will be conducted, using open-source intelligence if necessary. Any suspicions will be reported to the Compliance Officer, and the customer's risk profile will be updated accordingly. If necessary, an UTR will be raised.

Transaction monitoring is conducted on a risk-based approach, with more intense scrutiny applied when higher risks are identified.

Periodic Ongoing Monitoring and Review Frequency

Accounts shall be periodically reviewed from the date of the last CRA based on the customer's risk level:

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

The above time frames are a backstop for when an account review is required. If the customer triggers before and a review is conducted, the periodic review timer restarts and is set from the date of the last customer review.

Transaction Monitoring

Transaction monitoring is to be carried out in real-time by an internally generated system. Transaction monitoring shall be based on:

- Automated software (the transactions will be reviewed in real-time);
- Post transaction monitoring the depending on the risk assessment of the customer meaning the review frequency of the account holistically; and
- Triggers, rules and events.

As can be seen from the above, transaction monitoring is not only determined by the level of risk posed by the customer, but there are also triggers based on (but not limited to) if the customer is exceeding their expected level of activity as determined by the customer's profile IP changes, Large or complex transactions and on the rationale behind the activity of the customer.

Customer Screening

As a licenced entity, the Company recognizes the importance of the customer profile and has in place practices to comply with the laws and regulations in relation to, identification, verification and screening of new and existing customers for sanctions, political exposure and negative media.

The process being followed is that upon the customer's **first withdrawal** and consequently **upon reaching deposits of XCG. 4,000 (approximately €2,000), cumulatively lifetime or in one lump sum**, the customer will be immediately screened. Those customers who checks are dubious shall be passed on to the Compliance Officer for further verification. The Compliance Officer may appoint anyone working within the unit to investigate such matters. If such searches reveal a positive match, and the match has met several criteria, such match will be reported accordingly to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Jurisdiction
- Photo identification
- Identification or passport number

If such a match has been found, one should also investigate through open sources to obtain further information and immediately inform the Compliance Officer by following internal reporting procedures.

The Company reserves the right to request further documentation in relation to any possible match for which more documentation will be deemed necessary to verify such suspicion.

Politically Exposed Persons (PEPs)

A Politically Exposed Person means natural persons who are or have been entrusted with prominent public functions, other than middle ranking or more junior officials. The definition also covers their immediate family members or persons known to be close associates of such persons.

For the purposes of this definition the term "natural persons who are or have been entrusted with prominent public functions" includes the following:

- (a) Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries.
- (b) Members of Parliament or similar legislative bodies.
- (c) Members of the governing bodies of political parties.
- (d) Members of superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances.
- (e) Members of courts of auditors or of the boards of central banks.
- (f) Ambassadors, charges d'affaires and high-ranking officers in the armed forces.
- (g) Members of the administrative, management or supervisory boards of State-owned enterprises.

- (h) Anyone exercising a function equivalent to those set out in paragraphs (a) to (f) within an institution of the European Union or any other international body. Family members include the following
- (i) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
- (j) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
- (k) the parents of a politically exposed person;

Persons known to be close associates means:

- (a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
- (b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

When a customer is flagged as a PEP, or is a family member of a PEP, or is a person known to be a close associate to a PEP; in addition to the regular CDD measures applied on the account, further measures are undertaken. Such customers are classified as **high risk** as per this Policy.

Situations involving PEP require the application of EDD measures, independently of the outcome of the risk assessment. This entails having to determine whether a client is a PEP or otherwise and, should this be the case, apply of the following pre-established EDD measures:

- i. Obtain senior management approval to service the PEP;
- ii. Establish what is their source of wealth and, where applicable, their source of funds; and
- iii. Conduct enhanced on-going monitoring of the Account Holder's activity.

Client Risk Classification

Upon registration, the Company makes a risk classification for each Account Holder.

The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

The level of due diligence that should be performed on the Account Holder is determined based on the risk classification above.

The Monitoring of Account Holder activities

The Company takes reasonable steps to prevent activities of money laundering and terrorism financing and constantly monitors all Player activities including financial habits and behavior in order to mitigate industry related risks such as money laundering, terrorism financing and other criminal activities such as fraud.

Unusual activities

The Company has systems in place to monitor the activities on the Player Accounts for the presence of any unusual or suspicious. These activities include but are not limited to:

Duplicate or multiple Player Accounts

Any Player Accounts containing the same personal information, IP address or bank account is considered to be a duplicate account. It is not permitted for an Account Holder to have duplicate Player Accounts or manage more than one (1) Player Account when using the Services on the Website including but not limited to the web-based version. If the Company becomes aware, suspects or believes that this might be the case it reserves the right to immediately terminate any and all Player Accounts held and the Player Account balances either deemed as forfeited by the Account Holder in which event the deposit will be subject to further investigation by the Company. Any winnings arising from such behavior will be forfeited.

Collusion

Upon the suspicion of the multiple registration by Account holders acting in collusion or as a syndicate, the setup of fictitious Player Accounts or the use of front men, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close Player Accounts.

Identity fraud

At the detection of any use of falsified documentation (identity fraud), the Company will proceed to close the Player Account(s). Any winnings arising from such activities shall be confiscated and the amount deposited will be subject to further investigation.

Deposits and Withdrawals

All financial transactions must match the name of the credit card or other payment accounts through which the Player Account is funded, or money is withdrawn. Any inconsistencies will be considered a breach of the Terms and Conditions. The transaction will be suspended and the Player Account subject to further investigation.

Deposits

An Account Holder is only permitted to use its personal information and personal bank account. The information provided on the deposit form must be identical to the pertaining data held by the Company.

An Account Holder may deposit money in his Player Account only in order to play on the Website and use the Services and is not allowed to withdraw without prior wagering activity.

Furthermore, the Company will not grant interest on deposits. The Company reserves the right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Withdrawals

An Account Holder can only make a withdrawal request once the initial deposit amount is fully used, and specific bonus terms of a bonus must be satisfied before requesting its withdrawal.

No withdrawal will be processed, and funds cannot be withdrawn from the Player's Player Account until: (i) the required verification checks have been satisfactorily completed; (ii) payments have been confirmed; and (iii) the Player has complied with any other withdrawal conditions, specific rules and promotional terms relating to the Player's use of the Website and/or affecting his/her Player Account (for example, any applicable bonus terms), and (iv) wagering activity has been conducted by the Player in a minimum amount to be further determined by the Compliance function.

Withdrawal requests can only be addressed to the Account Holder registered on the Player Account and only to the account from which deposits were made. The information provided on the withdrawal form must be identical to the personal data held by the Company. Withdrawal requests made to other parties will not be taken into consideration.

Transactions using Cryptocurrency

In those cases where Player request's payment in Crypto, the following will be applicable.

Crypto 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..

Reporting Procedures (RP)

Suspicious activity or transaction

Suspicious activity is any customer activity that is outside of the ordinary, in other words activity that is not normal or expected activity given the customer's profile.

All suspicious activity must be investigated and given due consideration. Therefore, it is crucial that the Compliance Officer understand the customer profile, as this understanding is used to determine if there is knowledge, suspicion, or reason to believe that the business or customer is engaging in money laundering or terrorist financing activities.

Any unusual customer activity or transactions that are not commensurate with the established profile of the customer should be considered as a potential indicator of suspicious activity.

Following the detection of any potential suspicious activity, the subsequent investigations should establish the reasons for the unusual activity or transaction in order to either eliminate or confirm the suspicion raised.

Recognition of Unusual Transactions

An unusual transaction is one that deviates from a customer's typical behavior or profile. To identify such transactions, it is crucial to understand the customer's usual transaction patterns.

- **Key Factors to Recognize Unusual Transactions:**
 - **Inconsistent Activity:** Transactions that are inconsistent with the customer's established profile or business relationship.
 - **Complex, Large, or Unexplained Transactions:** Transactions that are unusually large, complex, or lack a clear lawful purpose.
 - **Suspicious Patterns:** Unusual patterns that could indicate potential money laundering or terrorist financing activities.

We must utilize both objective and subjective indicators, as outlined in the NORUT legislation, to evaluate whether a transaction qualifies as unusual. Staff should be well-trained to recognize these indicators, with all unusual transactions reported to the **Compliance Officer** for further review.

Documentation of Unusual Transactions

Once an unusual transaction is recognized, it is essential to document the transaction thoroughly, including any supporting documents (e.g., copies of identification, transaction records, etc.).

- **Key Steps for Documentation:**
 1. **Transaction Details:** Record the transaction's date, amount, payment method, and any relevant context (e.g., associated customer or business).
 2. **Supporting Documentation:** Collect and retain any documents related to the transaction, including customer identification documents, transaction slips, cash-out records, or any relevant correspondence.
 3. **Compliance Officer Review:** The Compliance Officer must ensure the transaction and its documentation are properly filed and stored for future reference.

All records related to unusual transactions must be maintained in a secure filing system by the Compliance Officer, ensuring that the necessary information can be easily retrieved for future assessments or external reports.

Reporting of Unusual Transactions

The reporting of unusual transactions is a critical part of compliance with AML/CFT regulations. We are obligated to report unusual transactions both internally (to the Compliance Officer) and externally (to the Curacao **Financial Intelligence Unit (FIU)**).

Internal Reporting

- **Immediate Action:** Once an unusual transaction is identified, it must be immediately reported to the Compliance Officer using the approved internal reporting form. The report should be thorough, including all relevant transaction details and any supporting documentation.
- **Compliance Officer Review:** The Compliance Officer will review the transaction, assess whether it raises suspicion of money laundering or terrorist financing, and determine if further action is needed.
- **Documentation:** Along with the report, all additional documentation related to the transaction (e.g., identification documents, transaction history, supporting evidence) must be submitted to ensure a complete record is kept.
- **Internal Recordkeeping:** The Compliance Officer must ensure that all reports and documents related to unusual transactions are properly documented and stored securely.

External Reporting

- **Reporting to the FIU:** If the Compliance Officer determines that the transaction is suspicious and meets the criteria for reporting, it must be submitted to the **Financial Intelligence Unit (FIU)** promptly. The FIU is the authority responsible for reviewing suspicious transactions and deciding whether further investigation is required.
 - **Method of Reporting:** Reports must be submitted via the **FIU's secure reporting portal**, with all relevant information about the unusual transaction, including the customer's details and transaction records. This ensures that the FIU has all necessary information to investigate the potential illicit activity.
 - **Urgency:** Reports must be submitted as soon as possible, without unnecessary delays, to meet the regulatory obligation. The compliance team should prioritize any report that involves substantial sums or seems to have links to criminal activity.
- **Acknowledgement by the FIU:** Upon submission of the report, the FIU will acknowledge receipt of the Unusual transaction report (UTR) and will notify the casino within 24 hours. If further information is required, the FIU will make a request, and the Compliance Officer will provide it promptly.
- **Follow-up:** If no response is received from the FIU within the required timeframe, the transaction may proceed, unless otherwise instructed by the FIU or the Compliance Officer. However, if additional information is requested, the Compliance Officer will coordinate with the necessary staff to ensure timely and complete responses.

Reporting Criteria

- **Transactions over XCG 5,000:** Any transaction involving an amount equal to or greater than XCG 5,000, regardless of the payment method, is considered for reporting.
- **Complex or Unusual Transactions:** Transactions that appear complex, large, or have no clear lawful purpose must be scrutinized and potentially reported.
- **Sanctioned Entities:** Transactions involving individuals or entities named in the Sanctions National Ordinance are automatically considered unusual and must be reported.

Once a report is submitted to the FIU, the Compliance Officer should record and maintain a copy of the report, along with any supplementary documents and correspondence with the FIU.

Tipping-Off and Prejudicing an Investigation

Tipping- Off

Tipping-off occurs when any personnel discloses the following to a customer or anyone outside the AML/CFT unit:

- That an Unusual Transaction Report (UTR) has been made to the Compliance Officer or submitted to the Financial Intelligence Unit (FIU).
- That information about the customer has been shared with the FIU.
- Any details related to ML/TF investigations or any information that could impact an ongoing investigation.

Tipping-off can happen before or after submitting a UTR. However, it is not considered tipping-off if personnel are discussing concerns with the Compliance Officer or submitting a UTR. Personnel are also not committing tipping-off if they are conducting normal customer inquiries or gathering information to assess suspicious activity, as long as they do not disclose any suspicions.

Prejudicing an Investigation:

Personnel will commit an offence if they disclose to any third party that an investigation is being conducted or is about to be initiated, potentially prejudicing the investigation.

Punishments for Tipping-Off and Prejudicing an Investigation:

- The offence can result in disciplinary action within the company, including immediate relief of duties.
- Fines and imprisonment are possible penalties, in line with Curaçao's broader AML/CFT regulatory framework, although specific penalties for tipping-off are not explicitly outlined in the laws. Sanctions can include administrative measures, fines, or criminal charges depending on the severity of the offence.

Exceptions:

It is not tipping-off if inquiries are made to gather further information to assess whether suspicion, knowledge, or belief of ML/FT exists.

It is also not tipping-off if you inform customers about their obligations under the AML/CFT regulations, such as providing them with terms of business.

Important: If any disclosure is necessary, it must be brought to the Compliance Officer for review to ensure compliance with legal requirements.

Employee Screening

It shall be the Company's policy that new employees are to provide the following:

- Passport or I.D.;
- Proof of address; and
- Police conduct.

The Company prior, to engagement, shall run a PEP & Sanction check on potential employees, and the individual shall also be duly requested to obtain references from previous employers.

A copy of the due diligence required shall be kept on file for individuals that are required to hold positions which must be approved. Such shall be carried out at a minimum annually for the duration of the employment.

The Company will monitor the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the Company's operations. Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the Compliance Officer, and should they wish to remain anonymous, this can be done via an anonymous letter.

Know Your Employee

The Know Your Employee ("KYE") assessment is based on the carrying out of interviews and the collection of certificates, references, identification documents (passport/identity card), and police conducts. The Company ensures

the suitability of the persons employed to carry out tasks relevant to the prevention of ML/FT through employee screening.

The analysis of the interview and the documents collected are used to decide on employment matters. As part of the KYP requirements, the KYE screening records and documentation obtained prior to the onboarding of the individuals is reviewed and maintained by HR every 2 years from the start of the individual's employment with the Company.

New employees would also need to undergo training. A probation period is applied where deemed appropriate so that the Company may, if necessary, take a quick action with regards to unsuitable persons operating with the Company's operations.

Employees Training

A key element of our compliance programme is ensuring that all employees are trained as to their compliance responsibility and developments in the area. The Company ensures that all individuals employed with the Company receive relevant training and information in order to fulfil the Company's obligations under the AML/CFT legislation.

The Company will develop ongoing employee training under the leadership of the Compliance Officer and senior management. The Company is obliged to provide training in relation to AML & CFT due to Compliance requirements. Such training is compulsory and shall be completed by every employee as soon as possible upon commencement of employment and shall be refreshed at least annually. Failure to do so without good reason constitutes a significant breach of their employment contract and may result in termination of their employment.

All employees, consultants and the Board of Directors receive continuous training in accordance with the following training plan. The training will be provided at different levels throughout the organization, for which all personnel shall be subject to at least a minimum level of understanding of AML/CFT and the internal policies concerning AML/CFT.

Additional specific training is provided to employees whose specific job in whole or in part is to oversee that no ML or FT occurs using the Company's services. This training will be more specific and role-focused e.g. the Payments Team may undergo further training regarding how to recognise AML transaction red flags the AML team will receive more in-depth AML training. Training will be tailored and updated based on the typologies and trends in the industry to ensure that all relevant staff are kept abreast of the AML/CFT landscape, both from a regulatory and business perspective.

All training provided to an employee, or which the employee participates in, shall be recorded within the Company's training records and provided upon request.

Periodicity

- On employee onboarding, within 3 months.
- Once a year for relevant persons including Senior Management and Board of Directors, or whenever there is new regulation or significant development, whichever comes first.

Scope

- Relevant parts of current/future regulations
- Relevant parts of the Company's business risk assessment
- Relevant parts of these guidelines and its related controls procedures

- Information to facilitate the detection of ML and/or FT, e.g. relevant judgements or sanctions decisions or trends, patterns or methods of ML and/or FT
- What to do when risks are identified, including how, when and to whom to escalate unusual customer activity or other red flags and, where appropriate, to report
- Exchange of experience on transactions reviewed during the year and of any transactions/activities reported to the police or FIAU
- The Company's record retention policy
- The disciplinary consequences for non-compliance with this Policy or applicable laws

Training Records

The training is documented, electronically or in paper form, with the following information:

- Content of the training
- Name of the participants
- Details of the trainer
- Date of the training

The Company conducts training either on a face-to-face basis or via electronic means, depending on the location of the participants.

Internal Auditing

The Company has outsourced its internal audit function to an independent third party, which is responsible for reviewing the internal guidelines, controls, and procedures for complying with Curaçao's **Anti-Money Laundering (AML)** and **Countering the Financing of Terrorism (CFT)** regulations. While the audit function is outsourced, ultimate responsibility for compliance lies with the Company.

The independent internal audit function regularly assesses whether the Company's:

- **Organizational structure, control processes, IT systems, models, and procedures** are appropriate and effective in managing AML/CFT risks.
- **Business activities** align with the Company's internal controls and guidelines.
- **Internal controls** are sufficient and effective for mitigating AML/CFT risks.
- **Other control functions** are reliable and assess the quality of the work being done.

The Company's AML/CFT policy is audited annually to ensure the ongoing effectiveness of internal controls and compliance with applicable regulations.

Based on the audit findings, the independent internal audit function provides recommendations to the relevant departments or individuals. The Company ensures that these recommendations are acted upon and implemented effectively to strengthen internal controls and mitigate potential risks related to money laundering and terrorist financing.

