

Anti-Money Laundering, Counter-Terrorism Financing and Counter-Proliferation Financing Policy

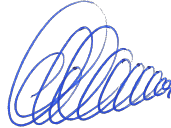
TECHWAVE B.V.

Curaçao, 2025

Document revision history

Revision	Date	Purpose	Responsible	Approver	Security
v 1.0.	30.05.2025	For internal service needs	Herman Theodorus Oosten Director	Raoul Armando Behr Director	Confidential

Approval

Version	Version Date	Approved By	Approval
V 1.0.	30.05.2025	Director	 

Contents

1.	DEFINITIONS.....	5
2.	POLICY STATEMENT	7
3.	APPLICABILITY AND REGULATORY FRAMEWORK.....	7
4.	DEFINITION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING	8
5.	POLICY IMPLEMENTATION	9
5.1.	THE COMPANY’S OBLIGATIONS	9
5.2.	APPOINTMENT OF A COMPLIANCE OFFICER.....	9
5.3.	RESPONSIBILITIES OF SENIOR MANAGEMENT	10
5.4.	EMPLOYEES’ RESPONSIBILITIES	10
6.	RISK-BASED APPROACH	11
7.	BUSINESS RISK ASSESSMENT	11
	SCREENING & CUSTOMER RISK ASSESSMENT.....	11
8.		11
8.1.	CUSTOMER RISKS.....	12
8.2.	CUSTOMER ACCEPTANCE POLICY	13
8.3.	DUE DILIGENCE	13
8.4.	ONGOING DUE DILIGENCE.....	14
8.5.	ENHANCED DUE DILIGENCE	15
8.6.	IDENTIFICATION	15
8.7.	RECORD KEEPING	16
8.8.	TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS.....	16
	REPORTING OF UNUSUAL MONETARY OPERATIONS OR TRANSACTIONS.....	16
9.		16
	RECOGNITION OF UNUSUAL TRANSACTIONS	16
9.1.		16
	REPORTING PROCEDURE	17
9.2.		17
9.3.	Reporting and Prohibition of Disclosure.....	18
10.	DATA STORAGE	19
11.	EMPLOYEE DUE DILIGENCE.....	19
12.	TRAINING	20

13.	INDEPENDENT AML AUDIT FUNCTION	21
14.	EXAMINATION BY THE CURAÇAO GAMING AUTHORITY	21
15.	INTERNATIONAL SANCTIONS	22
16.	OFFENCES AND SANCTIONS.....	22
17.	APPENDIX A	23
18.	APPENDIX B	24
19.	APPENDIX C	25

1. DEFINITIONS

"CGA"	Curaçao Gaming Authority
"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.
The "Company"	means TECHWAVE B.V. (company number 165403, registered address Emancipatie Boulevard Dominico F. "Don" Martina 31, Willemstad, Curaçao) which is a holder of license number OGL/2024/1676/0905 from the CGA.
"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.
"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"	include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens. 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).
"Politically Exposed Persons (PEPs)"	means: Foreign PEPs are 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. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, and the direct family members or close associates of such persons. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the

		board or equivalent functions, and the direct family members or close associates of such persons.
"Sanctions Ordinance"	National	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"		is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.
"Targeted sanctions"	financial	are measures imposed by governments or international bodies to restrict the financial activities of specific individuals or entities linked to unlawful activities, such as terrorism or money laundering. These sanctions aim to prevent these parties from accessing the financial system. Unlike general sanctions that apply broadly to entire countries, targeted sanctions focus on specific individuals or entities. This approach minimizes the impact on the wider population while addressing particular risks. Targeted financial sanctions apply to individuals or entities listed on sanctions lists maintained by organizations like the United Nations or the European Union.
"Unusual transaction"		A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.
"(Ultimate) ownership (UBO)"	beneficial	Refers to the natural person(s) who ultimately own(s) or control(s) 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.

2. POLICY STATEMENT

The Policy on Anti-Money Laundering and Counter-Terrorism Financing (hereinafter – “the Policy”) outlines the general unified standards and procedures of anti-money laundering and combating terrorism financing which must be adhered to by TECHWAVE B.V., (“the Company”) its directors, officers and employees.

In any country or jurisdiction where the applicable anti-money laundering and counter-terrorism financing laws and regulations require TECHWAVE B.V. to establish higher standards, such country standards must be adhered to.

Compliance with this Policy is mandatory and essential for ensuring that TECHWAVE B.V. is fully compliant with applicable anti-money laundering and counter-terrorism financing laws and regulations of respective countries and jurisdictions.

TECHWAVE B.V. is committed to an annual review and critical reassessment of this Policy considering the Company’s business strategies, goals and objectives on an ongoing basis.

TECHWAVE B.V. will always seek to disrupt this activity by cooperating fully with the authorities and reporting all unusual activity to the Financial Intelligence Unit.

3. APPLICABILITY AND REGULATORY FRAMEWORK

The Company is bound by the Government of the Country of Curaçao with regards to Anti-Money Laundering and Countering Financing of Terrorism (hereinafter – “**AML - CFT**”). The local authorities in charge of the supervision of AML - CFT matters for the gaming sector are Curaçao Gaming Authority (CGA) and the local Financial Intelligence Unit (“FIU”).

Curaçao online gaming industry is licensed and regulated under the National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92), and the National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99) and the FIU Curaçao which is the authority supervising adequate reporting of unusual transactions.

The following laws and regulations are applicable to the Company for the reporting of unusual transactions in Curaçao:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);

- Curaçao 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 also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering ("FATF") and the Guidelines and instructions of the European Commission as well as all six Directives of the European Union on AML and CFT.

The AML/CTF Policy applies to TECHWAVE B.V. and shall be communicated with all employees of the Company, as well as the subsidiaries and affiliated companies within the group to which TECHWAVE B.V. outsources some of its operations, to ensure they are aware of their responsibilities under AML/CTF regulations and the policies set out by the Company. For each version update, the Policy shall be communicated to its Employees and other Staff. The policy shall also be shared with any third party entering into a contract with the Company who has any access to transactional Customer data or information which might otherwise present Money Laundering and/or Terrorism Financing (hereinafter – "ML/TF") risks.

4. DEFINITION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Broadly, the international anti-money laundering provisions are aimed at requiring to:

- Identify Customers and unusual transactions at the placement and layering stages.
- Keep adequate records which should prevent the integration stage being reached and provide an audit trail for investigators.
- Report unusual activity or behavior to the relevant regulatory or legislative authority.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.

Proliferation financing involves providing funds or financial services that are used, either fully or partially, to develop, produce, acquire, or transport nuclear, radiological, biological, or chemical weapons and their delivery systems, in violation of national or international laws.

Specific typologies relevant to the gaming industry include the use of gaming accounts to deposit and withdraw funds without significant gameplay, structuring transactions to avoid reporting thresholds, and using third parties to place bets or claim winnings.

5. POLICY IMPLEMENTATION

5.1. THE COMPANY'S OBLIGATIONS

The measures, procedures and controls defined in this Policy are kept under regular review so that risks resulting from changes in the characteristics of existing clients, new clients and services are managed and countered effectively. The Policy is periodically (at least once a year) updated by the Compliance Officer based on the general principles set up by the Company's Director in relation to the prevention of Money Laundering and Terrorist Financing.

Main ML/TF prevention principles:

- The Company shall only carry on business with persons whom they have adequately identified and in whom there is no suspicion of criminal or terrorist activity.
- The Company shall undertake all measures at its capacity to not be used as a facility for laundering money or assisting others to do so intentionally or otherwise.
- The Company endeavors to verify the data supplied by the Customers upon registration and first withdrawal request, through methods and data available depending on country of residence.
- The Company must obtain reasonable information, adequately documented and corroborated, about the identity of all the Customers when required to do so under the remote gaming regulations.
- The Company shall take all measures necessary to detect and prevent fraudulent customers and activity through regular monitoring of Customer activity.
- The Company must not impede, by action or inaction, any official investigation of money laundering.
- The Compliance Officer must investigate, analyze, consult and, if appropriate, report the activity to the Financial Intelligence Unit Curaçao and take any other action considered legal and necessary.
- The Company shall, as much as possible, follow the relevant 40 + 9 recommendations of the Financial Actions Task Force (www.fatf-gafi.org).
- The Company shall follow all the laws and regulations relating to anti-money laundering and prevention of terrorism.
- The Company shall provide the necessary training for its employees in anti-money laundering, prevention of terrorism financing and fraud procedures.
- The Company shall keep records of all procedures carried out and reporting effected.

5.2. APPOINTMENT OF A COMPLIANCE OFFICER

TECHWAVE B.V. must designate an Compliance Officer who will be responsible for organizing the implementation of money laundering and/or terrorist financing prevention measures as specified in the Money Laundering Regulation and for liaising with the Financial Intelligence Unit Curaçao (FIU) Curaçao.

Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a Compliance Officer may be appointed as a Compliance Officer.

The Compliance Officer reports directly to the Board of Directors and has a dotted line of communication to the Chief Executive Officer (CEO). This structure ensures that the Compliance Officer has the necessary authority and independence to execute their responsibilities effectively. The Compliance Officer maintains direct lines of communication with senior management to ensure accountability and transparency. Regular reports on the status of the AML/CFT/CFP program, including any identified risks, compliance issues, and corrective actions, are provided to the Board of Directors and the CEO. The Compliance Officer also collaborates with other departments, as needed, to ensure a comprehensive approach to compliance.

The Compliance Officer obligations include but are not limited to:

- Establishment of appropriate internal control procedures with the purpose of prevention of monetary operations and transactions related to money laundering and/or terrorist financing: Customer and beneficial owner due diligence, submission of reports and information to the Financial Intelligence Unit Curaçao, storage of information according to Money Laundering Regulation, risk assessment, risk management (taking into account the type of product, service or transaction, geographical risk, etc.), compliance management and communication;
- Undertaking of appropriate measures so that their relevant employees and/or subcontractors are aware at all times of the provisions currently in force. Such measures shall include participation of the relevant employees and/or subcontractors in special ongoing training programs to help them recognize operations which may be related to money laundering and/or terrorist financing and provision of instruction to said employees as to how to proceed in such cases.
- Controlling overall compliance policy for prevention of money laundering and/or terrorist financing and ensuring adequate resources are provided for the proper training of staff and the implementation of risk systems.
- Keeping copies of all training materials. Updated AML training is given annually at minimum plus additional training when the need arises, for example in the case of significant changes in the Legislation. Records must be retained of all training sessions including dates, personnel, who received training (name, surname, functions in the Company, their signatures), Compliance Officer who trained staff (name, surname, functions in the Company, their signatures).
- Monitoring all amendments in the Legislation aimed at prevention of money laundering and/or terrorist financing and updating internal instructions according to up-to-date information. The internal instructions must be updated at least once a year.

5.3. RESPONSIBILITIES OF SENIOR MANAGEMENT

The Senior Management is responsible for:

- setting and approving the general principles underlying the Policy for Prevention and Combatting of Money Laundering, Terrorist Financing and the Financing of Proliferation
- appointing Compliance Officer and communicating to them the internal policies
- defining the duties and responsibilities of the Compliance Officer
- ensuring that effective and sufficient systems and controls are in place to enable compliance with all rules and regulations
- ensuring that the Compliance Officer have completed and timely access to all data required to effectively undertake their duties including, but not restricted to, data concerning customer identity, transaction documentation and other relevant information maintained
- ensuring that all employees are aware to whom they have to report any information concerning unusual transactions
- ensuring that the Compliance Officer have sufficient resources including competent staff and technological equipment
- assessing and approving the annual report and taking appropriate actions to remedy any weaknesses and/or deficiencies identified in the annual report.

5.4. EMPLOYEES' RESPONSIBILITIES

All TECHWAVE B.V. employees and/or subcontractors are responsible for considering the Policy and understanding responsibilities. All staff members must ensure that TECHWAVE B.V. procedures are adhered to and must obtain all documentary evidence as outlined within the Policy. In addition, employees and/or subcontractors must ensure that all unusual circumstances are immediately reported to Compliance Officer.

A dedicated 'Suspicious Transactions' email box has been created which is available to all employees and/or subcontractors (compliance@techwave.com). This mailbox is to be used for all employees and/or

subcontractors to report accounts they suspect of money laundering and/or terrorist financing, especially in the cases if behavioral triggers occur. All such unusual transactions shall be reported internally to the Compliance Officer.

6. RISK-BASED APPROACH

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/PF risks specific to the online gaming industry. When developing the 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.

To effectively apply the risk-based approach, the Company conducts a preliminary assessment of the risks associated with money laundering and terrorist financing within the organization, and based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

The Company shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. The Company shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

7. BUSINESS RISK ASSESSMENT

The Business Risk Assessment (BRA) framework is a crucial component of the Company'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.

The Company 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. The Board of Directors must formally approve the Business Risk Assessment (BRA) and risk appetite.

8. SCREENING & CUSTOMER RISK ASSESSMENT

For the purpose of identification, assessment and analysis of money laundering, terrorist financing and/or financing of proliferation risks related to Principal activity, TECHWAVE B.V. conducts risk assessment in accordance with "Customer Risk Assessment Guideline". The steps taken to identify, assess and analyze risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of TECHWAVE B.V.

Each customer shall be assigned a risk rating (low, medium, high) based on geographic, transactional, and behavioral risk factors. As a result of the risk assessment, TECHWAVE B.V. maintains the following risk classification:

- Low risk. Customers who are classified as Low risk are subjected to Standard Due Diligence procedures related to the request for Know-Your-Customer (hereinafter – "KYC") documentation and constant monitoring of activities on the account.

- Medium risk. If the customer fails to provide the requested documentation at a stage where this is required (i.e. when it has been requested due to defined triggers, like change in risk profile from low to medium/high, turns to become a PEP, starts requesting high volume transactions etc.), the account will be under increased monitoring.
- High risk. Customer activity is the determining factor for the classification of a customer as High-risk. Any Customer for which an automated alert has been generated or an inappropriate activity has been detected will be categorized as High-risk, for which an Enhanced Due diligence procedure is applied.

The Company shall assure “Business Risk Assessment Guideline” is up to date, reviewed and refreshed in the event of material changes to the risk environment.

AML screening is one of the methods used for risk assessment of the Company's existing or potential customers:

- The Company performs the screening of each customer, to identify high-risk clients and Enhanced Due diligence procedure is applied.
- When conducting the screenings, the Company seeks to achieve three main objectives:
 - Make a risk assessment.
 - Avoid violating sanctions.
 - Protection from regulatory fines.
- With AML screening, dedicated employees ensure that existing or potential Customers are not present in any of the sanctions lists, banned or wanted lists, are not classified as PEPs and do not have any adverse media data on file.
- The Company performs AML screening of its customers in the following cases:
 - Upon account opening and withdrawal requests.
 - As risk levels of Customers change over time.
- The Company should regularly, at least once per year, check the risk level of their Customers following their screening.
- To perform AML screening of any Customer, the Company is required to first obtain the full name and date of birth of the Customer.
- Then with the help of internal checks, the name of the person is screened against all sanctions and watch lists, to ensure that they are not listed in any of them.
- With access to global regulatory databases like watch lists, PEPs and sanctions data, these solutions increase the reliability of verification processes.
- Hence, these methods not only provide comprehensive risk control for the Company, but allow them to fulfill AML obligations effectively.

8.1. CUSTOMER RISKS

TECHWAVE B.V. does not allow anonymous gambling. Every player is required to register and identify themselves with TECHWAVE B.V., by providing their name, date of birth, address, and contact details. Further details of the KYC process are set out in Section, “Screening & Customer Risk Assessment”. A registered account is only allowed to be operated by the registered individual, and the Company does not allow third-party use of an account. The system is regularly scanned for links between accounts in the registered details.

Politically Exposed Persons (“PEPs”) and sanctioned individuals are not allowed as Customers. All Customers are checked using various methods and if a match is found, the account shall be blocked with immediate effect, to ensure we do not transact with any sanctioned individuals. Adverse media checks are also conducted regularly. Any match detected during these checks, where there is a high likelihood of being

a true match, shall be evaluated by the Compliance Officer to consider whether there is reasonable ground to submit a Unusual Transaction Report to the FIU.

The Company shall not rely solely on open-source information and shall make regular contact directly with any Customer identified as potentially risky to verify the Customer information provided and obtain further documentation where required.

8.2. CUSTOMER ACCEPTANCE POLICY

TECHWAVE B.V.'s Customer acceptance policy is based on what is required under law and in line with the Company's risk appetite and the risk assessment of the business. Certain types of individuals shall not be accepted as Customers, by either being prevented from registering or blocked from using our site:

- Under 18s (or 21 in some jurisdictions).
- PEPs. Politically exposed persons (PEPs) may be subject to pressure and vulnerable to corruption. We do not accept PEPs as Customers and shall block any such individual from registering or playing on our websites.
- Individuals on FATF, UN, EU, UK or OFAC sanctions lists (see **Appendix A & B** for the compiled list of banned/prohibited countries).
- Residents, in countries deemed to be high risk, to measure AML/CTF risk.
- Individuals where we have reason to suspect involvement in ML/TF or other types of criminal activity.
- Self-excluded Customers, excluded from our websites or any national self-exclusion register available within the license conditions.
- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent.
- Customers where an increased risk level in the Customer profile for any reason warranted us terminating the Customer relationship.

8.3. DUE DILIGENCE

Customers must be identified, and their identity may be verified prior to establishing a business relationship:

- When there are doubts about the veracity or authenticity of the previously obtained identification data of the Customer.
- In any other case, when there are suspicions that the act of money laundering and/or terrorist financing is, has been or will be carried out.
- Before establishing a business relationship with the Customer, TECHWAVE B.V. employees and/or subcontractors must apply the following due diligence measures:
 - Identification of a Customer and verification of the submitted information based on information obtained from a reliable and independent sources, including using means of electronic identification and of trust services for electronic transactions.
 - Verification of a Customer's residential address by request for provision of secondary document such as bank statement or utility bill showing residential address.
 - Verification of a Customer's e-mail address by sending a letter with verification link.
 - TECHWAVE B.V. shall be prohibited from establishing relationships without requesting the Customer to submit data confirming their identity, or where there is a substantiated suspicion that the data recorded in these documents is false or falsified.
 - TECHWAVE B.V. employees and/or subcontractors shall be prohibited from establishing or continuing relationships and carrying out transactions when it is not possible to fulfil the due diligence requirements established in this Policy:

- where, in the cases established by this Policy, the Customer fails to submit the data confirming his identity, or where he submits incomplete data.
- where the data are incorrect, where the Customer avoids submitting the information required for establishing his identity or the submitted data are insufficient for that purpose.

8.4. ONGOING DUE DILIGENCE

TECHWAVE B.V. must apply Customer due diligence measures not only in respect of new Customers but also in respect of existing ones, having regard to the level of risk, in the event of new circumstances or new information related to the determination of the level of risk posed by the Customer, their identification information, activities and other relevant circumstances.

Continuous monitoring is in place to track Customer behavior and where transactions are deemed to be unusual, further investigations are undertaken by the Compliance team. These investigations will include, but not be limited to, the following:

- Inactivity period followed by intense activity.
- Game type behavior and amounts played.
- Withdrawals amount against Deposits amounts.
- Transactional behavior.
- Payment method used.

During the period of cooperation with the Customer, TECHWAVE B.V. is obliged in all cases:

- To carry out the ongoing monitoring of the Customer's activity, used payment methods, including scrutiny of transactions undertaken throughout the course of such relationships, to ensure that the transactions being conducted are consistent with TECHWAVE B.V. knowledge of the Customer, risk profile as well as the source of funds.
- To ensure that the documents, data or information submitted by the Customer during due diligence are appropriate, relevant, regularly reviewed and kept up to date.
- To monitor the achievement of the threshold of Cg. 4,000 deposited into the Customer's account, whether in a single transaction or in several transactions that make up the specified amount. The Company calculates the Cg. 4,000 deposit threshold on the basis of a rolling period of 24 hours.
- TECHWAVE B.V. must pay attention to any activity which they regard as likely, by its nature, to be related to money laundering and/or terrorist financing, and in particular to complex or unusually large transactions and relationships or deposits/withdrawals with Customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist financing prevention measures are insufficient or do not correspond to international standards. TECHWAVE B.V. must examine the basis for and purpose of execution of such operations or transactions and the results of the investigation must be recorded in writing.
- TECHWAVE B.V. may, in accordance with internal policies and internal control procedures, refuse to execute the deposits/withdrawals and terminate the transactions or relationship with the Customer, where:
 - The Customer avoids submitting, or refuses to submit, additional information to the Company, at its request and within the specified time limits.
 - Where there is suspicions or substantial grounds to suspect that money laundering and/or terrorist financing was, is, or will be performed, or it has been attempted.
 - Where there are suspicions or substantial grounds to suspect that the Customer's funds have been obtained from criminal activity.
 - Where there is suspicions or substantial grounds to suspect that the transactions or activities are related to terrorist financing.

8.5. ENHANCED DUE DILIGENCE

Measures of enhanced customer due diligence goes beyond that of the CDD. Enhanced measures are warranted especially in cases identified as high risk. The checks shall cover (but not limited to):

- Unusual Transactions (see Business Risk Assessment Guideline).
- Customers located in a country that the Financial Action Task Force (FATF) deems sensitive.
- Politically Exposed Persons (PEP's).
- A person performing prominent public functions.
- A close associate of a person performing a prominent public function.
- Clients reached a threshold set in Section 8.4.
- Other Clients that the Company considers to be high-risk in accordance with Business Risk Assessment Guideline.

In the case of High-risk clients, TECHWAVE B.V. applies the following additional measures to effectively manage and mitigate its risks:

- Requiring the quality and extent of requisite identification data to be of a certain standard (e.g., documents from independent and reliable sources, certified documents, third person information, documentary evidence).
- Obtaining additional data and information from the Customer, where this is appropriate for the proper and complete understanding of their activities and source of wealth, source of funds.
- Screening against sanctions and government watch lists.
- Assessing the individual's history, reputation, and personal and professional background through review of public records – including civil, criminal and bankruptcy / insolvency records, identification of professional affiliations.
- Search for adverse media and internet research.
- Applying of ongoing monitoring of High-risk Customers' transactions and activities.

The Company shall use all reasonable efforts to obtain this information. All information should be checked against all available databases.

8.6. IDENTIFICATION

TECHWAVE B.V. identifies the Customer and retains the following data on the person:

- Name, surname.
- Personal identification code or, if not, the date and place of birth and the country of residence.
- Gender
- Date of birth (age).
- Customer's email address.
- Customer's address and phone number.
- Payment details.

TECHWAVE B.V. verifies the correctness of the data specified by the Customer, using information originating from a credible and independent source for that purpose. Where the identified person has a valid document specified above, or an equivalent document, the person is identified, and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

- Required proof of identity – must include copies of the following:

- Passport or Driving License or National Identity Card.
- Proof of Address – Utility Bill / Official or Bank Correspondence.
- Proof of ownership of the linked payment method – Bank Statement or Card Statement (figures may be blocked out).
- These documents shall be preferably sent in digital format signed with a person's own digital signature. TECHWAVE B.V. may ask for these documents also in notarized format (whereby the validity (originality) of the document is confirmed by the notary public).

In the event behavioral triggers (see the Business Risk Assessment Guideline) occur, TECHWAVE B.V. may ask from the Customer presentation of additional documents. In certain situations, it may be necessary to establish the source of funds and the wealth of the Customer, or ask for other information in respect of the nature of the transaction, aim of transaction etc. The Company shall use all reasonable efforts to obtain this information.

8.7. RECORD KEEPING

All due diligence performed, including the rationale for risk assessment levels assigned to customers, will be documented and maintained. The CDD process is aligned with identified risks, ensuring that due diligence efforts match the customer's risk profile. All risk mitigation measures are documented and utilized during ongoing monitoring to manage potential risks effectively. Records will include copies of identification documents, verification data, transaction details, and any correspondence related to the client's risk assessment and monitoring. Further information about the data policy of TECHWAVE B.V. can be found in Section "Data Storage".

8.8. TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS

If the customer cannot provide compliant documents within thirty (30) days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the Cg. 4,000 thresholds, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the 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.

All actions taken in response to non-compliant documents shall 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.

9. REPORTING OF UNUSUAL MONETARY OPERATIONS OR TRANSACTIONS

9.1. RECOGNITION OF UNUSUAL TRANSACTIONS

TECHWAVE B.V. must pay attention to any activity which they regard as likely, by its nature, to be related to money laundering and/or terrorist financing, and in particular to complex or unusually large transactions, and all unusual patterns of transactions which have no apparent economic or visible lawful purpose, and relationships or monetary operations with Customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist

financing prevention measures are insufficient or do not correspond to international standards. TECHWAVE B.V. must examine the basis for and purpose of execution of such operations or transactions and the results of the investigation must be recorded in writing.

TECHWAVE B.V. must report to the Financial Intelligence Unit Curaçao any unusual monetary operations or transactions.

The following transactions or intended transactions are deemed unusual:

- A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing of terrorism;
- An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 - A cashless transaction in the amount of Cg. 5,000.00 or more.
 - Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 - Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 - A cash out in the amount of Cg. 5,000.00 or more;
- Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Indicators (a) to (c) are referred to as "objective indicators", while (d) is referred to as "subjective indicator". While the objective indicators are based on measurable facts and do not require interpretation, automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behaviour of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

Additionally, linked transactions that cumulatively reach or exceed Cg. 5,000 within a 24-hour period are considered for unusual transaction reporting.

TECHWAVE B.V. must immediately submit to the Financial Intelligence Unit Curaçao all the information available to TECHWAVE B.V., which the Financial Intelligence Unit Curaçao requested in its enquiry.

Upon establishing that their Customer is carrying out an unusual monetary operation or transaction, TECHWAVE B.V. must suspend the operation or transaction disregarding the amount of the monetary operation or transaction.

9.2. REPORTING PROCEDURE

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the Compliance Officer upon identification, providing a brief description of the specific mitigating measures taken.

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 Unusual Activity Report to the Compliance Officer. This ensures that the employee's legal obligation to report is fulfilled.

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than twenty-four (24) hours after the transaction has been executed, using the Internal Unusual Activity Report form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) 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, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within forty-eight (48) hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than forty-eight (48) hours after the transaction has been executed.

9.3. Reporting and Prohibition of Disclosure

Where the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible money laundering or terrorist financing, the transaction or professional act shall be carried out or the official service will be provided, and a report will be submitted to the Financial Intelligence Unit:

- A report to the FIU is submitted via GoAML reporting portal (link to register in GoAML - <https://portal.fiucuracao.cw>).
- The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.

The structural unit of TECHWAVE B.V., a member of a management body and any employee are prohibited to inform a person about a report submitted on them to the Financial Intelligence Unit, plan to submit such a report or the occurrence of reporting as well as about any precept made by the Financial Intelligence Unit Curaçao or about the commencement of criminal proceedings. After a precept made by the Financial Intelligence Unit Curaçao has been complied with, TECHWAVE B.V. may inform a person that the Financial Intelligence Unit Curaçao has restricted the use of the person's account or that another restriction has been imposed.

The prohibition is not applied upon submission of information to competent supervisory authorities and law enforcement agencies.

The exchange of information must be retained in writing or in a form reproducible in writing for the next five years and information is submitted to the competent supervisory authority at its request.

TECHWAVE B.V., its employee, representative and/or the person who acted on its behalf are not liable for damage caused to a person or Customer participating in a transaction made in economic or professional activities, in performing a professional act or in the provision of a professional service:

- upon performance of duties and obligations arising from Anti Money Laundering and Terrorist Financing Prevention regulations in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit.
- in connection with the performance of the duty to report in good faith.

TECHWAVE B.V. establishes a system of measures ensuring that the employees and representatives of the Company who report of a suspicion of money laundering or terrorist financing to the Financial Intelligence Unit Curaçao are protected from being exposed to threats or hostile action by other employees, management body members or Customers of the Company, from adverse or discriminatory employment actions.

10. DATA STORAGE

TECHWAVE B.V. must keep a register of reports of unusual monetary operations and transactions specified in Section 6, "Reporting of Unusual Monetary Operations or Transactions" of this Policy.

TECHWAVE B.V. must keep a register of the Customers with whom transactions or relationships were terminated under the circumstances specified in Section "Enhanced Due Diligence" of this Policy or under any other circumstances related to violations of the Policy.

Register data shall be stored in electronic form for five years from the date of termination of transactions or relationships with the Customer.

Copies of the identity documents of the Customer, other data received at the time of establishing the identity of the Customer and account and/or agreement documentation (originals and/or copies of the documents) must be stored for five years from the date of termination of transactions or relationships with the Customer.

The correspondence with the Customer must be stored in paper or electronic form for five years from the date of termination of transactions or relationships with the Customer.

The documents confirming a monetary operation or transaction and data or other legally binding documents and data related to the execution of monetary operations or conclusion of transactions must be stored for five years from the date of execution of the monetary operation or conclusion of the transaction.

Records of the results of the investigation specified in this Policy shall be stored for five years in paper or electronic form.

Time limits for storage may be additionally extended upon receipt of a reasonable request from a competent institution.

TECHWAVE B.V. must store the personal data of staff referred to in Section "Employee Due Diligence" of this Policy for five years upon termination of employment, unless longer storage is required by applicable Labour laws and regulations in the country of residence of the employee.

11. EMPLOYEE DUE DILIGENCE

Employee due diligence is a procedure used to screen employees. The screening procedure aims to identify and minimize business exposure to the risk of money laundering and terrorism financing. For the avoidance of doubt, same procedures apply not only to the contractual employees of the Company, as per Labour laws and regulations, but also to the contactors and/or subcontractors of the Company.

An employee's due diligence is based on the risk assessment of the business and the roles within it. Any employee whose role means they might be able to facilitate money laundering or terrorism financing must be screened. This includes:

- Prospective employees before they are employed to such a position.
- Existing employees before they are transferred or promoted to such a position.
- To screen both current and potential employees the Company should:
 - identify them.
 - verify their identity
 - confirm their employment history (e.g., through references)
 - decide whether they are suitable for the position and do not pose a risk to the Company.

The Company shall take into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of staff.

Roles with duties that might make the employee a target for collusion with, or coercion by, criminal groups must be subject to a tougher check.

The Company must consider checking whether the employee:

- has a criminal record (e.g., through a police check).
- is or has been subject to any regulatory, court or legal action.
- has used bankruptcy laws to their own advantage.
- has lived in high-risk countries or regions.

12. TRAINING

In providing the specified categories of employees with the AML/CTF training, TECHWAVE B.V. shall take into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of staff. TECHWAVE B.V. shall, within the framework of the training, explain to staff the AML/CTF requirements and provide detailed information on the measures and activities the staff are expected to conduct within the framework of their responsibilities.

TECHWAVE B.V. shall develop and document a staff training plan which contains at least the following programs:

- An internal training program for staff, which uses internal training resources (hereinafter referred to as the “internal training”).
- An external training program for staff, which uses external training resources, including participation of foreign experts (a qualified person in the AML/CTF area) (hereinafter referred to as the “external training”).
- A training program for new employees (employees who have just started to perform their duties or changed position at TECHWAVE B.V. (hereinafter referred to as the “new staff training”).

TECHWAVE B.V. shall ensure that the information on the conducted staff training is saved by documenting the following data:

- Name of the training.
- Personal data of the trained employee.
- Position and structural unit of the trained employee.
- Training venue.
- Head and organizer of the training.
- Time of training.
- Duration of the training.
- Result of knowledge tests and certificate obtained, if any.

TECHWAVE B.V. shall update the training programs in line with any modifications in internal and external regulations and supply of training programs in the market (for provision of external training).

TECHWAVE B.V. shall, at least once a year, assess compliance and efficiency of the training programs and make any necessary changes thereto.

TECHWAVE B.V. shall ensure that, in addition to the internal and external training, any employee may obtain the necessary advice from senior employees involved in the AML/CTF risk management.

TECHWAVE B.V. shall conduct an appropriate training program before new staff start to perform their duties. In addition to the internal training, TECHWAVE B.V. shall ensure extraordinary staff training in AML/CTF issues at least in the following cases:

- New internal and external regulations governing the AML/CTF have come into force and are applicable to the staff of TECHWAVE B.V.
- New products and/or services have been introduced which cause changes in the AML/CTF risk exposure.
- During the performance of his/her duties an employee violates the internal and external regulations governing the AML/CTF due to insufficient knowledge.

13. INDEPENDENT AML 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 and 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.

14. EXAMINATION BY THE CURAÇAO GAMING AUTHORITY

The Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the CGA 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.

15. INTERNATIONAL SANCTIONS

TECHWAVE B.V. shall be prohibited to perform any actions the performance of which is prohibited by the international sanctions implemented in Curaçao.

Prospecting Customers from countries that pose high ML/TF risks which lie outside of the business risk appetite shall be blocked from registration and/or login. The Compliance department reviews the list of accepted countries on a regular basis, in line with certified and credible sources of information regarding the level of ML/TF risks, corruption, political unrest, and countries subject to sanctions (see Appendix A for the compiled list of banned countries), embargos or similar measures, countries with no or little AML Regulations and monitoring by FATF, or countries providing funding and/or support for terrorism.

TECHWAVE B.V. shall be prohibited to accept transactions the execution of which would conflict with international sanctions implemented in Curaçao. Such transactions concluded after the establishment of the implementation of international sanctions:

- In the manner prescribed by this Law shall be null and void, and invalid.
- The fulfilment of the obligations which appeared prior to Curaçao establishment of implementation of international sanctions in Curaçao must be terminated immediately or suspended for the duration of the implementation of international sanctions. It shall be prohibited to assume new obligations the fulfilment of which would conflict with international sanctions implemented in Curaçao.
- Upon the restriction of availability of accounts to the entities with respect to which international sanctions are implemented, expenses associated with routine holding of such accounts may be deducted from them, and interest as well as payments due under transactions, concluded prior to the commencement of the implementation of international sanctions, may be added only if any deductions or additions shall not be made available to the entity with respect to which financial sanctions are implemented.

16. OFFENCES AND SANCTIONS

If the Company does not comply with the compulsory AML/CFT requirements, it is committing an offense, which is an unlawful and punishable act.

The way in which an offence is punished depends on the severity of the offence committed. Offences are subdivided into misdemeanors and felonies.

Felony refers to a serious offence committed for which the lawbreaker will be tried, judged and sentenced by a court in Curaçao and Sint Maarten.

The penalty amount or fine for the various offences is specified in the National Ordinance Reporting Unusual Transactions (NORUT) (PB 2017, nr 99) and the National Decree Penalties and Fines Service Providers (ND PFSP) (NG 2010, no. 70).

The Central Bank will report an offence to be criminally investigated or prosecuted by the law enforcement in circumstances where the offender emphatically refuses to comply with the NORUT and/or NOIS.

Before proceeding to imposing a fine, the Central Bank shall inform the (financial) institution or individual in writing of its intention to impose a fine, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term.

17. APPENDIX A

Below is the compiled list of countries and jurisdictions identified as presenting AML/CFT strategic deficiencies. This list is primarily derived from:

1. The Financial Action Task Force (FATF) publications, including the *Call for Action (Black List)* and *Jurisdictions under Increased Monitoring (Grey List)*;
2. The United Nations Security Council Sanctions Lists, including countries or regions subject to targeted financial sanctions;
3. The European Union and the Kingdom of the Netherlands Consolidated Sanctions Lists, which are applicable to Curaçao; and
4. Guidance and alerts issued by the Curaçao Gaming Authority (CGA) or FIU Curaçao regarding high-risk jurisdictions or new restrictive measures.

This list is **not exhaustive** and may be updated when any of the above sources are amended or when new jurisdictions present AML/CFT or proliferation financing concerns

- | | |
|------------------------------------|----------------|
| ● Barbados | ● Laos |
| ● Algeria | ● Lebanon |
| ● Angola | ● Libya |
| ● Belarus | ● Mali |
| ● Bolivia | ● Monaco |
| ● Bulgaria | ● Mozambique |
| ● Burkina Faso | ● Myanmar |
| ● Cameroon | ● Namibia |
| ● Central African Republic | ● Nepal |
| ● Côte d'Ivoire | ● Nigeria |
| ● Côte d'Ivoire | ● North Korea |
| ● Croatia | ● Russia |
| ● Cuba | ● Somalia |
| ● Democratic Republic of the Congo | ● South Africa |
| ● Eritrea | ● South Sudan |
| ● Guinea Bissau | ● Sudan |
| ● Haiti | ● Syria |
| ● Iran | ● Tanzania |
| ● Iraq | ● Venezuela |
| ● Kenya | ● Vietnam |

* Contested territories that are not internationally recognized:

- Eastern Ukraine
- Transdniestria
- Crimea/Donetsk/Luhansk (Ukraine)
- Abkhazia
- South Ossetia

18. APPENDIX B

Below is the compiled list of countries/jurisdictions that are subject to limitations of the applicability of TECHWAVE B.V.'s license; however, it is not exhaustive and might also include other countries/jurisdictions that fall under these markets and/or license applicability restrictions.

- Afghanistan
- American Samoa
- Aruba
- Australia
- Belgium
- Belize
- Bonaire
- Bosnia and Herzegovina
- Botswana
- Burma
- Burundi
- Central African Republic
- Curaçao
- Democratic Republic of the Congo
- Eritrea
- Estonia
- France
- French Guyana
- Greenland
- Guadeloupe
- Guam
- Holy See (Vatican City)
- Iraq
- ISIL and Al-Qaida
- Ivory Coast
- Lebanon
- Libya
- Lithuania
- Marshall Islands
- Martinique (FR)
- Netherlands
- Occupied Palestinian Territory
- Poland
- Puerto Rico
- Qatar
- Republic of Guinea
- Republic of Guinea-Bissau
- Russian Federation
- Saba
- Saint Barthelemy
- Saint Martin
- Saint Pierre and Miquelon
- Somalia
- South Africa
- St. Eustatius
- Sudan
- USA
- US Minor Outlying Islands
- US Virgin Islands
- Venezuela
- Zimbabwe

19. APPENDIX C

Player Risk Matrix

Risk Rating	Nature	Location	Source of funds/Wealth	Transaction Size
Prohibited	Sanctioned individual and PEPs. A Customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements	Closed jurisdictions A Customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements Named on FATF's Blacklist	Cash A Customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements. Funds appear to be generated or linked to the proceeds of crime	A Customer that has breached any of the below thresholds but does not comply with the Company's CDD/EDD requirements.
High	Professional Gambler Customers that are sporting professional betting on sports High net worth individuals	Countries with AML/CFT strategic deficiencies	Use of over 5 different payments methods	Deposit or withdrawal of EUR 10,000 in any period
Medium	Public profile raises some form of concern e.g., adverse media, social media activity	Named on FATF's List B. Countries which in the opinion of the Compliance Officer represents heightened risk		Deposit or withdrawal or over EUR 3,000 (or currency equivalent) or aggregate in excess of EUR 3,000 (or currency equivalent) in a 30-day period
Low	Individual	Fully compliant with FATF No AML/CFT concerns	Bank transfer Debit or credit card Approved payment service provider	Under any of the qualifying payment thresholds

TECHWAVE B.V. _AML _ CFT Policy

V.1.0_reviewed

Final Audit Report

2025-08-29

Created:	2025-08-29
By:	Naomi Clifton (naomi.clifton@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAJSFu6P77h2CWjLZ9apYe0sf305FOh5DU

"TECHWAVE B.V. _AML _ CFT Policy V.1.0_reviewed" History

-  Document created by Naomi Clifton (naomi.clifton@hbmgroup.com)
2025-08-29 - 4:01:04 PM GMT
-  Document emailed to Annesol Melaria (annesol.melaria@hbmgroup.com) for signature
2025-08-29 - 4:01:11 PM GMT
-  Document emailed to Bryon Finies (bryon.finies@hbmgroup.com) for signature
2025-08-29 - 4:01:11 PM GMT
-  Email viewed by Annesol Melaria (annesol.melaria@hbmgroup.com)
2025-08-29 - 6:25:07 PM GMT
-  Document e-signed by Annesol Melaria (annesol.melaria@hbmgroup.com)
Signature Date: 2025-08-29 - 6:26:00 PM GMT - Time Source: server
-  Email viewed by Bryon Finies (bryon.finies@hbmgroup.com)
2025-08-29 - 7:34:02 PM GMT
-  Document e-signed by Bryon Finies (bryon.finies@hbmgroup.com)
Signature Date: 2025-08-29 - 7:34:23 PM GMT - Time Source: server
-  Agreement completed.
2025-08-29 - 7:34:23 PM GMT