

InterStorm (Curacao) N.V.

AML/CTF/CPF Policy

This document contains the policy and procedures the Company will undertake in running its online business. The contents of this document are confidential and are not to be reproduced without the express permission of the Company in any way. Any unauthorized copying, disclosure or distribution of the material in this document is strictly forbidden.

Version: 2.3
Date: 14/05/2025

Revision History

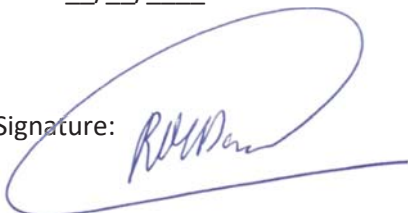
Version #	Date Issued	Approved By	Comments
1.0	August 2017	Carmanco N.V, Managing Director	Prepared by the MLRO
1.3	June 2020	Richard M. Dagelet (Director)	Reviewed by the MLRO
1.4	August 2021	Richard M. Dagelet (Director)	Reviewed by the MLRO
1.5	August 2022	Richard M. Dagelet (Director)	Reviewed by the MLRO
1.5	September 2023	Richard M. Dagelet (Director)	Reviewed by the MLRO (no changes)
2.0	January 2024	Richard M. Dagelet (Director)	Reviewed and updated by the MLRO
2.1	July 2024	Richard M. Dagelet (Director)	Reviewed and updated by the Compliance Officer to comply with the updated AML/CFT/CFP Regulations, published May 20,2024
2.2	February 2025	Richard M. Dagelet (Director)	Reviewed and updated by the Compliance Officer. (Responsibilities of the Compliance Officer and the MLRO are merged to match the terminology used by GCB)
2.3	May 2025	Richard M. Dagelet (Director)	Reviewed and updated by the Compliance Officer. (Internally reported unusual transactions added as a reason for termination of business relationship to Section 8.3)

Document Version 2.3 approved by

Richard M. Dagelet, Director

Date: 27/05/2025

Signature:



Contents

REVISION HISTORY	2
1. INTRODUCTION.....	5
1.1 PURPOSE	5
1.2 SCOPE	5
1.3. STATUS OF THIS DOCUMENT	5
1.4 REFERENCES	6
1.5 DEFINITIONS, ACRONYMS AND ABBREVIATIONS	6
2. POLICY STATEMENT AND AML COMPLIANCE PROGRAM	8
3. MONEY LAUNDERING / TERRORIST FINANCING / PROLIFERATION FINANCING. OVERVIEW.....	9
3.1 MONEY LAUNDERING AND PROCEEDS OF CRIME – DEFINITION AND STAGES	9
3.2 WHAT IS TERRORIST FINANCING?	10
3.3 WHAT ARE SANCTIONS?.....	10
3.4 WHAT IS PROLIFERATION FINANCING?	11
4. RESPONSIBILITIES OF THE COMPLIANCE OFFICER	11
5. FITNESS AND PROPRIETY.....	13
5.1 COMPANY’S OBLIGATIONS AND DUTIES OF THE EMPLOYEES	13
5.2 EDUCATION AND TRAINING	13
5.3 EMPLOYEE DUE DILIGENCE	14
5.4 INDEPENDENT AUDIT FUNCTION	15
6. THE RISK-BASED APPROACH AND MANDATORY HIGH-RISK SITUATIONS.....	16
6.1 RISK-BASED APPROACH.....	16
6.2 ML/TF/PF BUSINESS RISK ASSESSMENT AND IDENTIFIED RISKS	17
6.3 CUSTOMER RISK ASSESSMENT (CRA).....	18
6.4 TECHNOLOGICAL DEVELOPMENTS RISK ASSESSMENT.....	20
6.5 MANDATORY HIGH-RISK SITUATIONS.....	20
6.5.1 Politically Exposed Persons (PEPs)	20
6.5.2 Sanctioned (Designated) Individuals	22
6.5.3 High-Risk and Non-Reputable Jurisdictions	22
7. CUSTOMER DUE DILIGENCE	23
7.1 RISK-BASED CUSTOMER DUE DILIGENCE	23
7.2 CUSTOMER DUE DILIGENCE MEASURES	23
7.2.1 Identification and Verification of the Customer	24

7.2.2 Identification and Verification of the Beneficial Owner	26
7.2.3 Obtaining Information on the Purpose and Intended Nature of the Business Relationship	27
7.2.4 Ongoing Monitoring.....	27
7.3 ENHANCED DUE DILIGENCE AND ENHANCED ONGOING MONITORING	29
<u>8. APPLICATION OF THE CUSTOMER DUE DILIGENCE MEASURES</u>	<u>31</u>
8.1 APPLICATION AND TIMING OF CDD / EDD MEASURES.....	31
8.2 INABILITY TO COMPLETE CDD MEASURES	32
8.3 TERMINATION OF BUSINESS RELATIONSHIP	32
<u>9. FUNDS MANAGEMENT</u>	<u>33</u>
<u>10. REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS</u>	<u>33</u>
10.1 UNUSUAL TRANSACTION REPORTING	33
10.2 INTERNAL REPORTING PROCEDURE	34
10.3 INTERNAL EVALUATION AND EXTERNAL REPORTING	35
10.4 PROHIBITED AND PERMISSIBLE DISCLOSURES.....	36
<u>11. RECORD KEEPING PROCEDURES</u>	<u>36</u>
11.1 RECORDS TO BE RETAINED AND RETENTION PERIOD.....	37
11.2 RETRIEVAL OF RECORDS	38
<u>APPENDIX 1. RED FLAGS</u>	<u>39</u>
<u>APPENDIX 2. SOURCE OF WEALTH/FUNDS DECLARATION.....</u>	<u>42</u>
<u>APPENDIX 3 – INTERNAL SAR/STR TEMPLATE.....</u>	<u>43</u>

1. INTRODUCTION

1.1 Purpose

The purpose of the AML/CTF/CPF Policy is to lay down the Company's approach towards anti-money laundering, combating the funding of terrorism and proliferation financing; and generally, detail the internal practices, measures, procedures and controls relevant to the prevention of Money Laundering, Terrorist Financing and Proliferation Financing. The other Policies and Procedures, dedicated to specific areas of AML/CTF/CPF are prepared based on the principles set by this Policy.

The AML/CTF/CPF Policy aims to assist the directors, senior management and the employees of the Company in understanding and fulfilling their obligations under the applicable local legislation, international treaties, conventions and other legal instruments, thus ensuring an effective implementation of the provisions of all applicable Laws, rules and Regulations.

The AML/CTF/CPF Policy has been issued in order to achieve the following main purposes:

- to provide an understanding of ML/TF/PF threats and risks the Company is exposed to;
- to outline the requirements set out in all applicable Law, rules and Regulations;
- to provide an overview of procedures and explain the risk-based approach adopted by the Company;
- to explain the duties and responsibilities of senior management, the Compliance Officer and others, including employees, which are relevant to the prevention and detection of ML/TF/PF risks;
- to provide a better understanding of high-risk situations and customers' categories (including PEPs and sanctioned individuals);
- to explain the reporting procedure;
- to explain CDD and EDD measures, the timeframe of their application and the hybrid approach adopted by the Company;
- to lay down the main principles of the AML/CTF/CPF Training Program.

1.2 Scope

The AML/CTF/CPF Policy applies to all employees of the Company and also to all customers who want to establish business relationships with the Company and to use its services, provided under the Business to Customer (B2C) Remote Gaming License awarded by the relevant authority, which includes the following branch:

- **ShangriLa.com**

1.3. Status of this Document

This document was approved by the Director of InterStorm (Curacao) N.V.

The document will be reviewed and amended from time to time if necessary but at least once a year to ensure that it remains harmonized with amendments to legislation and other material developments originating from changes in international standards, especially those emanating from the regulated markets.

Any changes, updates or additions to this document have to be approved by the director of the Company.

The Policy shall be communicated by the Compliance Officer to the relevant employees of the Company that manage, monitor or control in any way the customers' transactions and activities and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein. Everyone in the Company, to varying degrees depending on their role, are required to be familiar with the contents of this AML/CTF/CPF Policy.

1.4 References

The main sources of the Policy are:

- National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (NOIS), PB 2017, no. 92);
- National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (NORUT), PB 2017, no. 99);
- Ministerial Regulation Indicators for Unusual Transactions (Ministeriele regeling indicatoren ongebruikelijke transacties, PB 2015, no. 73);
- Regulation for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (Applicable for Curacao casinos and providers of other online games), last updated January 2025;
- Sanctions National Ordinance (N.G.2014, no.55)
- Kingdom Sanction Act (N.G. 2016, no.54)
- FATF (Financial Action Tasks Force) Recommendations and Guidance
- GCB Requirements for Compliance Officer based on NOIS/NORUT

1.5 Definitions, Acronyms and Abbreviations

For the purposes of this Document, unless the context shall prescribe otherwise:

"AML/CTF/CPF" stands for Anti-Money Laundering, Countering Terrorist Financing and Combating Proliferation Financing.

"Business Relationship" means the provision of the gaming services which the Company is licensed to provide to individual customers.

"Beneficial Owner" of the account means the individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

"CDD" means Customer Due Diligence.

"CRA" means Customer Risk Assessment.

"Customer" means any natural person aiming to enter a Business Relationship or conduct a single or multiple transactions with the Company.

"Company" means InterStorm (Curacao) N.V.

“EDD” means Enhanced Due Diligence, advanced verification measures for high-risk customers and high-risk situations.

“FATF” means the Financial Action Task Force – the inter-governmental body responsible for setting the international standards for anti-money laundering (AML) and countering terrorist financing (CTF).

“FIU” stands for the Financial Intelligence Unit Curacao.

The **“Law”** means Acts and Regulations mentioned in the “References” section.

“ML/TF/PF” stands for the Money Laundering, Terrorist Financing and Proliferation Financing.

“Politically Exposed Persons (PEPs)” means any individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, as well as family members and known close associates of such individuals.

“Proliferation Financing” means the act of providing funds or financial services for use (in whole or in part) in the manufacture, acquisition, development, export, transshipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.

“SOF” means Source of Funds and relates to how the funds used for a particular transaction were obtained by the customer (e.g., transfer from the bank account owned by the customer or someone else, loan, winnings from the other companies).

“SOW” means Source of Wealth – is the origin of the customer’s entire body of wealth (e.g., ownership of the business, employment, investments, inheritance).

“RBA” means Risk-Based Approach, an approach that allows the Company to allocate resources directed proportionately in accordance with the extent of the ML/TF/PF risks posed, so that the customers posing the highest risks receive the highest attention meeting regulatory needs while effectively combating ML/TF/PF.

“Regulations” means Regulation for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (Applicable for Curacao casinos and providers of other online games) that came into effect from May, 15th, 2024.

“SAR/STR” stands for Suspicious Activity Report / Suspicious Transaction Report.

“Senior Management” means directors, C-level officers and other managers of the Company with sufficient knowledge of the Company’s money-laundering and terrorist financing risk exposure and of sufficient authority to take decisions affecting the Company’s risk exposure.

2. POLICY STATEMENT and AML COMPLIANCE PROGRAM

The Company recognizes the importance of preventing potential money laundering, proliferation financing and terrorist financing activity and its responsibility to keep financial crime and any other unlawful activity out of gambling.

To this end the Company is committed to implement a comprehensive AML Compliance Program to ensure that the Company is protected against money laundering and stays in full compliance with relevant laws and regulations. The Company intends to do the following:

- 1 To appoint a competent **Compliance Officer** who will develop and oversee the implementation of the AML Compliance Program; verify the Company's compliance with law and Regulations; regularly review compliance with internal policies and procedures and report to the Director and senior management on a regular basis; oversee day-to-day compliance with the AML/CFT/CPF Policies and procedures, including implementation of due diligence and transaction monitoring, review of internal SARs, investigation of unusual transactions and reporting to the FIU if necessary, providing support and training to all relevant employees.
- 2 To develop adequate **AML/CTF/CPF Policies, procedures, CDD and EDD measures and controls**;
- 3 To ensure that the policies, procedures and controls for managing money laundering and terrorist financing risks, including the detection of criminal spend, are kept under **regular review** and their effectiveness is monitored and regular evaluated;
- 4 To adopt a **risk-based approach** in identifying and mitigating the ML/TF/PF risks;
- 5 To ensure that **adequate due diligence performed on customers** and on all **relevant employees**;
- 6 To perform an **ongoing monitoring** of customers' transactions and activities;
- 7 To ensure that any **suspicious transaction** is brought to the Financial Intelligence Unit's attention, as required by Law and that all other appropriate actions are taken to prevent and mitigate ML/TF/PF;
- 8 To ensure that the details of a customer relationship or individual transaction are preserved for eventual assessment by the FIU and other law enforcement and relevant authorities;
- 9 To develop and implement an **AML Training Program** for all relevant employees in the Company to raise awareness and improve knowledge among staff;
- 10 To **keep records** of any actions taken and of the reasons for these decisions;
- 11 To establish an **Independent Audit Function** to test the AML program.

The senior management is committed to this Policy and will ensure that the Compliance Officer has sufficient resources and the level of authority required to fulfil their duties effectively.

3. MONEY LAUNDERING / TERRORIST FINANCING / PROLIFERATION FINANCING. OVERVIEW

3.1 Money Laundering and Proceeds of Crime – Definition and Stages

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

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

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

- Placement;
- Layering;
- Integration.

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

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

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

The definition of money laundering goes beyond generically expounding the notion of money laundering on the basis of the three traditional stages identified above. In fact, passive possession of criminal property is also considered to amount to the offence of money laundering.

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

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

3.2 What is Terrorist Financing?

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

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

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

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

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

3.3 What are Sanctions?

Sanctions are political and/or economic prohibitions imposed by various national and supranational institutions against individuals, organisations or countries which prohibit any person from engaging in a specific activity (such as trade) with sanctioned entities.

Sanctions may be imposed for a variety of reasons, including preventing nuclear proliferation, human-rights violations, preventing the escalation of war, drug trafficking, terrorism, and more.

Useful links:

- 1 [EU Sanctions Map](#) (updated by the EU Commission)
- 2 [The European Union Sanctions List](#)
- 3 [The UN Sanctions List](#)
- 4 [The Office of Foreign Assets Control \(OFAC\) list](#)
- 5 [Curacao Local Sanctions List](#)

3.4 What is Proliferation Financing?

The Proliferation Financing means the act of providing funds or financial services for use (in whole or in part) in the manufacture, acquisition, development, export, transshipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.

The issue of proliferation received international attention for several years. A number of international conventions provide for measures to detect and prohibit proliferation, especially with regard to nuclear materials (such as the Nuclear Non-Proliferation Treaty). These treaties do not, however, consider the aspect of financing proliferation. In 2004, the UN Security Council issued Resolution 1540, requiring states to put in place a number of measures in order to prevent the proliferation of nuclear, chemical or biological weapons. Subsequently, the FATF started in 2007 to consider the threats related to proliferation financing and its interconnection with terrorism and terrorism financing.

The interconnection is based on the fact that proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing.

Identifying, assessing, and understanding proliferation financing risks on a regular basis is essential in strengthening a country's or private company's ability to prevent designated persons and entities involved in Weapons of Mass Destruction (WMD) proliferation from raising, storing, moving, and using funds, and thus other financial assets.

4. RESPONSIBILITIES of the COMPLIANCE OFFICER

The Compliance Officer shall lead the Company's Anti-Money Laundering Compliance Program and report to the Director and senior management at least annually.

The Compliance Officer is a second line of defence in the detection, prevention and mitigation of ML/TF/PF and falls under the company's Legal & Compliance Department. The role of the Compliance Officer includes the following non-exhaustive list of responsibilities:

- Advising the Company on compliance with requirements emanating from applicable laws, regulations and licence requirements;
- Evaluating risk and advising the Company on risk mitigation in matters relating to AML/CTF/CPF from all angles of the group's business activities and across all relevant markets and jurisdictions, including for new territories, products and verticals, funding methods and customer bases;
- Developing, maintaining and reviewing policies and procedures as mandated by regulatory requirements relating to AML/CTF/CPF;
- Ensuring that the policies and procedures are implemented correctly and as necessary to deal with amendments to applicable laws, regulations and licence requirements and to take into account changes to the company's corporate structure, business activities, geographical territories, products and/or services offered, customer base, and any other changes to its setup;
- Ensuring that proper and sufficient due diligence is performed on customers and their activities as well as all third parties with which the group engages in the carrying out of its business activities. Monitoring the controls in place and verifying whether these are being communicated and implemented in practice in an effective and timely manner;
- Establishing and maintaining adequate and proper record-keeping, logging and reporting procedures within the Company;
- Identifying any weaknesses in the system;
- Receiving internal reports on possible instances of money laundering or terrorism financing to determine whether sufficient grounds exist for the submission of a Suspicious Report to the Financial Intelligence Unit and taking any and all other necessary actions;
- Devising and executing an ongoing Training Program for the Company, ensuring that all employees are aware of their legal obligations, of the risks associated with ML/TF/PF, of the internal reporting mechanisms in place, as well as providing updates and information to the Company on AML/CTF/CPF to improve awareness and knowledge among at all levels;
- Acting as the main point of contact and relationship manager with licensing authorities, institutions and bodies in all relevant jurisdictions, including without limitation the Curacao Gaming Control Board, FIU, the Executive Police and the law courts in Curacao and their equivalent in all other jurisdictions and markets which are relevant to the business activities of the Company.

Any findings and shortcomings noted by the Compliance Officer are to be reported to the Director and senior management together with recommendations on their elimination, prevention or mitigation.

The Compliance Officer shall have access to all relevant information necessary to perform his/her duties and enjoy sufficient seniority and command to be able to act independently of management.

The Compliance Officer shall have the necessary knowledge of the Company's activities, services and products and the ability to take decisions on whether internal reports are to be escalated to the FIU and what information to provide to the FIU without undue influence or coercion from the Company's management.

The Compliance Officer shall take ultimate managerial responsibility for AML issues, but this does not diminish senior management responsibility and accountability for AML.

5. FITNESS and PROPRIETY

5.1 Company's Obligations and Duties of the Employees

Individual employees face criminal penalties if they are involved in money laundering or terrorist financing.

In terms of applicable Law, individual members of staff (and in particular, directors as well as employees in certain instances) may face administrative sanctions for contraventions of AML/CTF/CPF obligations or criminal penalties if they are involved in money laundering or the funding of terrorism, or if they breach their non-disclosure obligations under the Law and Regulations.

To this end the Company shall take appropriate measures from time to time and at least annually to:

- Ensure that employees are aware of relevant AML/CTF/CPF legislation and data protection requirements, as well as adopted AML/CTF/CPF measures, policies, controls and procedures;
- Provide training in relation to the recognition and handling of transactions that may be related to proceeds of criminal activity, ML and TF;
- Carry out screening of relevant employees appointed, both before the appointment is made and during the course of the appointment.

5.2 Education and Training

The content and effectiveness of the training provided is critical to the success or failure of the Company's AML/CTF/CPF strategy. Properly trained staff is fully aware of the very real risks of ML/TF/PF, and shows more confidence in the identification of unusual transactions and riskier situations that may turn out to be suspicious. It is important that staff is made aware of the regulatory obligations and ML/TF/PF risks the Company is exposed to.

The Training Program has to be targeted and tailored for specific roles and departments and to have a different structure for new employees, existing employees and for different departments of the Company. Ongoing Refreshment training shall be given at regular intervals so as to ensure that employees are reminded of their duties and responsibilities and kept informed of any new developments.

The training form will vary from online training and regular updates on ML/TF/PF topics via email to classroom training sessions.

It should be noted that awareness and training should be provided to employees and other Company officials whose duties include the handling of either relevant financial business or relevant activity, irrespective of their level of seniority. The list of "relevant employees" includes:

- Directors;
- Senior Management and Heads of Departments;
- the Compliance Officer;

- Employees of Legal & Compliance Department;
- Members of AML Team;
- Employees of Financial and Payment Department
- Audit Staff;
- Members of Customer Support Team.

The Company must ensure that in all of its contractual undertakings with outsourced service providers (if applicable), it obliges third party service providers to submit their employees, staff, agents and other personnel to adequate AML/CTF/CPF training.

The Training Program should include, without limitation, the following:

- a) General understanding and knowledge about ML/TF/PF;
- b) Examples of high-risk situations and red flags indicating potential ML/TF/PF activities;
- c) New trends or changes in the industry and technology that can impact the Company and increase the ML/TF/PF risks;
- d) Relevant provisions of the Law and Regulations;
- e) Individual and Corporate responsibilities and obligations under the Law and the applicable offences and penalties;
- f) Defense against prosecution and how to avoid committing “tipping off” offence;
- g) CDD / EDD measures;
- h) Record-keeping procedures;
- i) Reporting procedure and the role of the Compliance Officer;
- j) Risk management procedures, including CRA, internal controls, compliance management and the employee screening procedure;
- k) Knowledge about AML/CTF/CPF policies and procedures adopted by the Company.

For more detailed description refer to the separate [“Staff Training Policy and Training Program”](#) document.

5.3 Employee Due Diligence

The Company needs to ensure that the ‘key employees’ placed in positions of responsibility are fit and proper.

For the purpose of this document “fit and proper” entails satisfaction of the following criteria:

1. Honesty, integrity and reputation;
2. Competence and capability; and
3. Sound financial standing.

For the above-mentioned individuals, the integrity check will be performed at the stage of signing the employment contract. The integrity check involves an assessment of an individual’s criminal record or past involvement in civil or regulatory investigations or proceedings.

To determine that the prospective employee is of high honesty, integrity and of good reputation, the following matters will be considered:

- Whether the person has been or has reason to believe that he/she may be investigated for a criminal offence or any other proceedings by a competent authority;
- Whether the person has been charged with a criminal offence;
- Whether the person has been convicted of any criminal offence;
- Whether the person has been the subject of any civil suit;
- Whether the person has a tainted regulatory performance record with any competent authority;
- Whether the person has been publicly criticised for any function.

In the event of finding that a potential key employee has been convicted of a relevant offence, each case will be considered on its individual facts and merits and consideration will be given to the seriousness, relevance and date of the conviction. Additionally, a due diligence check will be performed on a prospective key employee including obtaining copies of the identification documents, police conduct certificate, media and online search. In some cases, references from the most recent two previous employers might be requested.

During the course of employment, the on-going screening will be conducted from time to time (e.g., when duties and roles of the employee change or at any other time at the Company's discretion).

The Company will ensure that the relevant training is provided to all key employees to keep them informed of developments in gambling legislation or any guidance, issued by supervisory authority relevant to their role.

Key Persons must take all reasonable steps to ensure that the way in which they carry out their responsibilities in relation to licensed activities does not place the Company in breach of its license conditions.

5.4 Independent Audit Function

The Auditing Function is the third and final line of defence in the company's ML/TF/PF detection, prevention and mitigation tools and measures. The purpose of the independent Audit Function is to monitor and evaluate the existing AML Compliance Program. The Audit Function must be independent and performed by people not involved in the Company's day-to-day operations or not from AML compliance team. The Audit Function has to be sufficiently qualified to ensure that their findings are reliable.

The following obligations of the Audit Function are addressed specifically for the prevention of ML/TF:

- Reviewing and evaluating, at least on an annual basis the appropriateness, effectiveness and adequacy of the policy, practises, measures, procedures and control mechanisms applied for the prevention of ML/TF/PF mentioned in the Policy;
- Reviewing and evaluating work of the Compliance Officer;

- Performance of transaction testing, assessment of training adequacy, interview of AML team, sampling of unusual transactions and their evaluation, assessment of the adequacy of the record retention system;
- Determining whether the Policy has been effectively implemented in a timely manner, identifying any gaps in the implementation of the Policy and recommending measures for their elimination, prevention or mitigation;
- Presenting reports and making recommendations to the Directors and senior management on the company's technical and regulatory compliance and the implementation of the Policy.

Findings and observations of the Auditor, in relation to point above, shall be submitted, in a written report form, to the Director and senior management, together with any recommendations.

6. The RISK-BASED APPROACH and MANDATORY HIGH-RISK SITUATIONS

6.1 Risk-Based Approach

The principle behind the Risk-based Approach (RBA) of the Company is that resources should be directed proportionately in accordance with the extent of the ML/TF/PF risks posed, so that the customers posing the highest risks receive the highest attention and dedication of resources. The application of the risk-based approach should ensure that measures to prevent or mitigate ML/TF/PF are commensurate with the risks identified and that resources are allocated in the most efficient ways. High risk areas should be subjected to enhanced procedures, whilst simplified or reduced controls may be applied in areas of low risk.

As regulatory requirements and risks always change, the Compliance Officer shall monitor and evaluate, on an ongoing basis, the effectiveness of the measures and procedures of the adopted RBA. The Compliance Officer shall also be responsible for the development and implementation thereof, of all the other policies, procedures and controls according to the framework of the adopted RBA.

A risk-based approach requires the full commitment and support of senior management, and the active cooperation of all employees.

The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the Company. These steps require to:

- identify the money laundering and terrorist financing risks that are relevant to the Company and its operations;
- design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- monitor and improve the effective operation of these policies, procedures and controls;
- record what has been done, and why.

6.2 ML/TF/PF Business Risk Assessment and Identified Risks

The effectiveness of Risk Management depends on the proper understanding of the ML/TF/PF risks to which the Company is exposed.

To this end the Company performs ML/TF/PF Business Risk Assessment (BRA). The main purpose of the BRA is to identify and assess the Company's ML/TF/PF threats and vulnerabilities and evaluate identified risks to determine priorities for addressing them.

The following risk factors/risk areas have been considered by the Company while performing its ML/TF/PF BRA:

- a. information about the risks, made available to the Company by the supervisory and regulatory authorities, National and Supranational Risk Assessment Results and other reputable sources;
- b. industry experience of the Compliance Officer and other senior managers;
- c. risk factors relating to:
 - i. its customers;
 - ii. the countries or geographical areas, in which the company operates;
 - iii. the types of products and/or services it offers;
 - iv. the transactions which take place in connection with the provision of the products and services it offers;
 - v. the means of payment which it accepts from its customers;
 - vi. the delivery channels used to provide its goods and services;
 - vii. any identified internal risks which it is exposed to;
 - viii. any identified TF risks which it is exposed to;
- d. internal statistical information where available.

Where risks have been identified, mitigating measures will be devised and implemented where they are not already in place. Subsequent reviews of the risk assessment will ascertain how effective the mitigating measures have been in minimizing AML/CTF/CPF risk and revise processes where appropriate.

Business Risk Assessment is formulated in separate document. The Company also implements a **Jurisdiction Risk Assessment** that periodically assesses the geographic risk faced by the Company.

The information gathered from the Business Risk Assessments and the Jurisdiction Risk Assessment is utilized to feed into the **Customer Risk Assessment (CRA)**. The CRA evaluates the risk exposure of each individual customer after assessing all the risk factors available. This approach allows the Company's employees to focus their attention on higher risk players.

The most common risk factors across all brands and jurisdictions are the following:

1. Customer Risk

- Perpetrators of identity theft and identity fraud
- PEP customers and sanctioned individuals
- High spenders
- Disproportionate spenders
- Multiple accounts opened by bonus abuse "syndicate"

- Accounts with Beneficial Owner where it transpires that there is a mismatch between the details provided and the actual origin and/or ultimate beneficiary of player funds
 - Accounts with unauthorized access (account takeover)
- 2. Geographical Risk**
- Customers with connections through their nationality, place of birth, residence and work to high-risk/non-reputable jurisdictions
 - Customers using payment methods that have been funded or issued from high-risk jurisdictions
 - Customers with financial transactions to/from high-risk jurisdictions
 - Account activity from high-risk jurisdictions
- 3. Product/Service/Transactional Risk**
- Criminal spends
 - High volume of transactions
 - Deposit and withdrawal without playing
- 4. Interface Risk**
- Identity fraud and identity theft
 - Multiple users of one account
 - Non-face-to-face transactions
 - Use of the gaming account unauthorized by the real account holder use of the gaming account
- 5. Means of Payment Risk**
- Customers using third party payment instruments, with or without the owner's permission, including stolen or hacked payment instruments
 - Multiple payment methods used by a customer, preventing not a closed deposit-withdrawal loop
 - Customers requesting to withdraw funds to an account in a different payment institution or different country.
- 6. Internal/Employee Risk**
- Lack of AML/CTF/CPF knowledge and/or lack of AML/CTF/CPF training
 - Lack of adequate and relevant due diligence checks of employees
 - Inadequate AML Policies, Procedures and Controls
 - Collusion between employees and players
 - Misuse of test accounts and other forms of unauthorized access
 - Lack of automation and an excess reliance on manual checks and manually-generated reports
- 7. Terrorist Financing Risk**
- Customers – subjects of adverse media, linked to terrorist groups
 - Customers from terrorist-related jurisdictions

6.3 Customer Risk Assessment (CRA)

Customer Risk Assessment is an assessment of the particular risks the Company is exposed to in providing its services or products in the course of a business relationship to specific customers linked to particular jurisdictions. The extent to which a customer exposes the Company to money

laundering and terrorist financing risks have to be assessed at the commencement and throughout the duration of the business relationship.

The information collected to draw up the CRA will formulate **the Customer Risk Profile**.

On the basis of the CRA, the proper level of CDD can then be applied, as stipulated in this AML/CTF/CPF Policy and Customer Acceptance Policy.

The AML/CTF/CPF Policy recognizes four types of customer risk level:

- Low Risk
- Medium Risk
- High Risk
- Extreme Risk

Identifying a customer as presenting a higher risk of ML/TF/PF, does not necessarily mean that the customer is involved in ML/TF/PF. On the other hand, identifying a customer as carrying a lower risk of ML/TF/PF does not mean that the customer presents no risk at all.

The initial CRA is carried out immediately upon registration, when customers are screened against the PEP and Sanctions database. However, a comprehensive profile might become evident only after the relationship begins, and a customer starts transacting through the account. The constant monitoring of customer behavior allows to amend customer risk ratings accordingly and apply additional due diligence measures if it is required.

When assessing the risks, posed by a customer, the Company bears in mind the risk factors, that have been identified during the BRA and reconsiders them in view of the particular circumstances presented by the customer. The customer's reputation, nature and behavior also need to be factored in.

Here is the explanation of the above-mentioned factors:

1. Reputation

- a. Whether a customer has been a subject of adverse media linking him/her to crime (especially financial crime) and/or terrorism. It is advised to consider such reports from reliable and independent sources.
- b. We also need to consider situations, when a customer has already been a subject of our own Internal Suspicious Report, since such customers pose a higher risk.

2. Nature and Behavior

- a. The Customer is reluctant to provide any documentation and/or information requested by us for verification.
- b. The documents provided give rise to doubts as to their veracity or authenticity.
- c. The customer's transactions are unusually large or have an unusual or unexpected pattern.
- d. Links to high-risk countries or/and non-reputable jurisdictions.
- e. A customer with high deposit amounts, but his residential address shows that the customer lives in low-cost accommodation with no known source of income but nonetheless is spending money well above their apparent means.

While performing a Customer Risk Assessment, first, the personal characteristics of a customer (age, type, reputation, relationship duration) and customer's financial and betting behavior have to be considered; then the other factors (verification level, geographical risk and risks connected to the payment methods) have to be looked at to see how they affect the risk level of a customer. Employees therefore need to remain vigilant and use their experience and common sense in applying the company's risk-based criteria and rules, seeking guidance from their Compliance Officer.

Customer Risk Assessment is performed for each customer at different stages. More detailed explanation of the Customer Risk Assessment process is given in [“CAP and Customer Risk Assessment Process”](#).

6.4 Technological Developments Risk Assessment

The Technological Development Risk Assessment is a specific risk assessment that is performed in the following instances:

- A new product or service is offered;
- A new delivery mechanism becomes available;
- A new or updated technology is used for new or existing products.

The Technological Development Risk Assessment will take place prior to the launch of new products or services and prior to the implementation of new delivery mechanism or new technologies. This is done to determine whether the ML/TF/PF risk for new innovations are still within the Company's Risk Appetite. Such Risk Assessment must be documented and presented to the Director and senior management.

6.5 Mandatory High-Risk Situations

Independently of the risk assessment carried out by the Company, there are certain instances that are still deemed to be high risk.

6.5.1 Politically Exposed Persons (PEPs)

A PEP as **an individual who is or has been entrusted with a prominent public function, other than middle ranking or more junior officials, for the duration of their function up and until one year after they leave office (while in the case of family members and associates, these are no longer considered as PEPs immediately after the PEP leaves office)**, including the following individuals:

- 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 the 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, chargé d'affaires and other high-ranking officers in the armed forces;
- g) members of the administrative, management or supervisory boards of state-owned enterprises; and
- h) anyone exercising a function equivalent to those set out in paragraphs (a)-(f) above within an institution of the European Union or any other international organisation.

This list is by no means exhaustive and when making a decision if a particular customer could be considered as a PEP, the jurisdiction, type, size, budget, powers and responsibilities associated with a particular public function have to be taken into consideration.

The **family members of a PEP** are (but are not limited to):

- the spouse, or any person considered to be the equivalent to a spouse;
- the children and their spouses, or persons considered to be the equivalent to a spouse; and
- the parents.

The close associates are:

- a) a natural person known to have:
 - joint beneficial ownership of a body corporate or any other form of legal arrangement;
 - or any other close business relations with that PEP.
- b) a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.

Relationships with PEPs may represent increased risks due to the possibility that individuals holding such positions may misuse their power and influence for personal gain or advantage, or for the personal gain or advantage of close family members and close associates.

Such individuals may also use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position or resulting from bribery and corruption. In addition, they may also seek to use their power and influence to gain representation and/or access to, or control of, legal entities for similar purposes. Certain PEPs in certain positions may also be exposed to the possibility of being involved in FT.

The internal process is the following:

1. As soon as an account is created and first deposit is made, a screening is performed. The Company uses a software called **Dilisense** (<https://dilisense.com/en>) to screen all new customers against PEP databases.
2. If a PEP match is detected, an alert is immediately sent via email to the Compliance Officer, who is responsible to check whether the person is actually a PEP, or whether the hit was a false positive.
3. If the hit results in a positive match, the account shall be suspended, and shall not be re-opened until EDD has been done and senior management approval is granted.

4. For the purposes of this policy, the senior manager in charge of approving the PEP as a customer shall be the Head of Online Operations. The Compliance Officer shall assess the activity of the PEP, and after EDD is conducted, will consider the risks of money laundering, especially those relating to bribery and corruption. If the player activity is not suspicious, the Compliance Officer may, in its discretion, recommend to approve the customer. If the Compliance Officer and the Head of Operations agree not to accept the Customer, then the account shall be closed, and the Compliance Officer will be required to consider submitting Suspicious Activity Report to the FIU Curacao.

6.5.2 Sanctioned (Designated) Individuals

In any case, the Company will not do business with any entity or an individual where this would mean engaging with someone who appears on any sanction lists, or who is based in a country which is under sanctions, not least because this poses a particular risk in terms of receiving funds from terrorism.

We will take measures to ensure that people who attempt to access our services from sanctioned countries are blocked from doing so.

To ensure that there are measures aimed at combating terrorism, terrorist financing and the financing of the proliferation of weapons of mass destruction, the Company has the following procedures in place:

1. The initial screening of all new customers is done via an external tool (**Dilisence**) against EU, UN, OFAC and Local Curacao lists; and if there is a possible match an alert is immediately sent via email to the Compliance Officer, who are responsible to check whether the person is actually a designated individual, or whether the hit was a false positive.
2. The account in question and all funds (if any) or any transactions in the account must be blocked without any notice to the customer.
3. A Report must be sent to the FIU Curacao and the Company will await further instruction on how to proceed.
4. No funds should be returned to the designated person unless a license is granted by the relevant authorities, as this would be a breach of the financial restrictions.
5. The Compliance Officer will also consider if an external SAR/STR has to be submitted.

The procedure and the obligations related to the Sanctioned Individuals is an important part of every AML/CFT training.

6.5.3 High-Risk and Non-Reputable Jurisdictions

Under the AML Regulations the Company is required to have procedures in place to manage the risks posed by the countries and geographical areas where it operates and/or is exposed to as a result of its business activities. The jurisdictions, where the Company is offering its services or from where it receives money, have to be assessed on whether they are to be regarded as non-reputable or high-risk jurisdictions.

A **non-reputable jurisdiction** is one that has deficiencies in its national AML/CFT regime or has inappropriate and ineffective measures for the prevention of ML/TF/PF. The List on Non-Reputable Jurisdictions is based on the FATF “grey” and “black” lists.

The AML Regulations do not prohibit the establishment of a business relationship with customers from non-reputable jurisdictions but require the application of commensurate EDD measures, targeted to mitigate ML/TF/PF risks associated with that particular jurisdiction. To this end, a daily check is run to identify customers from high-risk jurisdictions and to act accordingly.

The Compliance Officer updates the High-Risk Jurisdiction list on a regular basis and informs the AML team about the changes.

7. CUSTOMER DUE DILIGENCE

7.1 Risk-Based Customer Due Diligence

Customer Due Diligence (CDD) is an integral part of the Risk-Based Approach. It involves gathering information about the customer in order for the Company to assess the extent to which the customer exposes it to money laundering and terrorist financing risks. CDD measures apply to the customers on a risk-sensitive basis depending on the type of customer, the business relationship or the nature of the transactions or activity.

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

CDD measures also assist the Company to determine whether a customer falls within its risk appetite as well as to understand the customer’s business profile with sufficient clarity to be able to conduct effective monitoring, including by identifying those transactions that fall outside this profile and thus consider whether there is a suspicion of ML/TF/PF or of proceeds of crime.

The methodology that has been adopted by the Company, requires to perform standard CDD and monitoring in Low and Medium Risk cases; and EDD and enhanced on-going monitoring in cases of High Risk.

The objective of risk-based customer due diligence is to ensure that, as the risks within the business relationship increase, so the level of information obtained and verified increases proportionally. Customers’ behaviour will be monitored continuously and risk ratings updated accordingly and in real time automatically in the back-office.

More information about the Company’s internal Customer Due Diligence Procedure, accepted documents, transaction monitoring process can also be found in separate documents “[Customer Acceptance Policy](#)” and “[Verification and Withdrawal Manual](#)”.

7.2 Customer Due Diligence Measures

The CDD normally consists of four measures:

1. Identification and Verification of the Customer;
2. Identification and Verification of the Beneficial Owner;
3. Obtaining Information on the Purpose and Intended Nature of the Business Relationship;
4. Ongoing Monitoring.

7.2.1 Identification and Verification of the Customer

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

Upon registration the following personal details of a customer are collected:

- a) Name and Surname;
- b) Date of Birth;
- c) Full residential address;
- d) Email address;
- e) Phone number;
- f) Username and password.

At this stage, information is also gathered such as IP address and DeviceID.

During the registration, the personal data entered by a prospective customer is cross-referenced with the already registered details in order to prevent customers from registering duplicate accounts with the same brand. In cases when duplicate details (Name / Surname and Date of Birth) are detected, such accounts are blocked straight after registration and customers are advised to contact customer support and to use or to re-activate the previously registered account. Accounts are also screened manually to detect similar details or possible duplicates on a daily basis.

According our Terms and Conditions customers *“may only open one account per person, per household, per IP address or device”*.

We do not allow the use of false names or the opening of an account for and on behalf of someone else. In cases where we detect an email address which already exists in our system, a customer is notified in real time and asked either to contact customer support and locate the previous account or to provide another email address.

In order to corroborate the location of a customer and for ongoing monitoring purposes, the back office constantly checks IP logins so we can use this information for internal investigations.

The Company uses a combination of on-entry and threshold CDD approach, or a so-called hybrid approach. The identification of the customer and the screening against PEPs and Sanctions database commence immediately upon establishing a business relationship (registration).

A customer must also confirm that his/her age is over eighteen (18) as minors are not allowed to register, accept our current Terms & Conditions and our Privacy Policy. Players who are not registered will not be allowed to deposit funds and/or to play.

Verification is triggered at the earliest of the following triggers:

- Customer reaches a transaction threshold of €2000 (the threshold is calculated on a daily basis taking into account all financial transactions - deposits and withdrawal - from the start of business relationship);
- When the withdraw method is different from the deposit method;
- The 3rd party payment method was used;
- Customers have changed their registered address;
- Customer is from the high-risk country / non-reputable jurisdiction;
- Any other suspicious cases and any customers who are deemed to be of high risk.

Once the threshold of €2000 has been reached, both deposit and withdrawal option for the account shall be locked until all requested verification documentation has been provided by the customer. If the requested documentation is not provided within 30 days, or if the customer refuses to provide the information, then the account shall be blocked, and the Compliance Officer will consider to file an STR.

Documentary Evidence

In verifying the identity, address and payment method of a customer, the Company shall request any of the following documentation:

Proof of Identity:

- Valid Passport;
- Valid Driving Licence;
- Valid National Identification document;
- Residence Permit.

Proof of Address:

- A recent utility bill for a service installed and provided at a residential property (except mobile phone bills);
- A recent bank statement or reference letter from a financial institution;
- An official conduct certificate issued by an authority of the customer's current place of residence where the customer has resided for the past 6 months;
- A recent bill / statements / appointment confirmation from the state hospital;
- A lease agreement;
- Other government-issued documents.

Proof of Payment:

This is requested unless proof of readily able to be provided directly by the payment institution.

- Bank documentation showing customer's complete IBAN and personal details;

- A colour photo of the card (both sides) with covered middle part of the card number and hidden CV2 number;
- A screenshot from the e-wallet account (e.g., Neteller / Skrill / Ecopayz).

Documents that are sent for verification purposes must be clear, legible and of good quality.

Documents submitted as proof of address should be dated within the last 3 months showing the full document with all four corners visible.

If unsure of the authenticity, the AML team should ask the customer to have the document certified by an independent professional, clearly indicating that they have verified the document, and including the date, certifier's name, surname, capacity/designation/profession, contact details and stamp (where available).

Identification documents in languages we cannot understand can't be accepted and verified by us. In cases when documents are in Chinese/Arabic/Cyrillic letters refer to the team member who can verify them. Leave a note, that the verification has been done by the colleague, who has confirmed the information. In all other cases, request another document from the customer in Latin letters.

7.2.2 Identification and Verification of the Beneficial Owner

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

"Beneficial Owner" of the account means the individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

The Company fully understands its responsibility to identify and verify the identity of the beneficial owner in circumstances where it transpires that there is a mismatch between the details provided and the actual origin and/or ultimate beneficiary of player funds.

In order to decide on what actions and what documents we need to request from a customer and a beneficial owner, it is important to understand the reasons and the circumstances surrounding such accounts, as the risk level differs. To this end the following measures are recommended:

- a) Requesting an explanation from a customer;
- b) Requesting verification documents from a customer and from a beneficial owner (ID, proof of address and proof of payment ownership);
- c) Search in the customer database across all brands to identify previous accounts or links;
- d) Assessing of the ML/TF/PF risk level or responsible gambling risk;
- e) Withdrawing remaining funds back to the original payment method and removing the third-party payment method from the back office;
- f) Advising customers to use the account only for himself/herself and getting confirmation that they understand and agree with this rule.
- g) Termination of business relationship in cases, when we believe that the registered account holder is not in control of the account and/or the risks are too high.

7.2.3 Obtaining Information on the Purpose and Intended Nature of the Business Relationship

The purpose behind the opening of a gaming account is usually self-evident. Customers want to open an account to play.

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

- Analyze the customer's deposit patterns – usual amounts, frequency of deposits, preferred payment methods.
- Check logins and IP to ensure that they are consistent and match the customer's registered location.
- Perform a background check – social media, open-source intelligence.
- Use statistical data from Government Statistics Department such as average national income and average disposable income but also internal data collected by the Company during its operations.
- Establish SoW as well as the expected level of activity.
- Analyze communication with the customer to see if there are indications of suspicious behavior or responsible gambling issues.
- Send a questionnaire to a customer (in conjunction with our social responsibility policy and procedure) to get information about their intended financial activity and their overall financial situation.

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

Source of Wealth (SOW) – is the origin of the customer's entire body of wealth (e.g., ownership of a business, employment, inheritance, investments). Taking into consideration the risk-based approach, the extent of the information that the company collects to verify SoW of a customer varies. In low-risk cases, the background check on social media and the average profile of a customer from a particular jurisdiction may be sufficient. In high-risk situations the information needs to be supplemented by documentation (see next section 7.2.4 and 7.3).

7.2.4 Ongoing Monitoring

The main purpose of this CDD measure is to ensure that:

1. Documents, data and information of a customer held are up-to-date;
2. Transactions are consistent with the company's knowledge of the customer and the customer's business and risk profile.

In cases when the documents held on file reach their expiry date, there is a procedure in place to request new documents from the customer.

Where we notice that a customer's activity is not in keeping with what we know or expect from the customer (e.g., activity cannot be justified on the basis of a customer's SoW or not in keeping with

the average profile or account activity noted to date or activity does not reflect a customer's usual transactional patterns), customer is asked to provide explanation and where necessary to provide SoF confirmation.

Each risk situation/risk indicator adds points to the overall score and the increase in overall score will prompt the AML team to review the account in question again.

Besides, there are several deposit thresholds that will result in account review by a member of the AML team and when SoF / SoW documentation may be requested:

- 2500 Euro single deposit (customers are from high-risk jurisdictions)
- 20 000 Euro deposit life-time
- 50 000 Euro deposit life-time

Source of Funds (SoF) relates to how the funds used for a particular transaction were obtained by the customer. As long as a transaction falls within the profile of the customer and the regular or expected activity carried out through one's account, there is no need for us to obtain specific information and documentation on the same; it is only where a transaction presents a departure from the known or expected behavior of a customer that the company is required to question the same. It is crucial to understand the reason for such divergence and obtain sufficient information and documentation on the matter.

The following is a list of SoW/SoF documents that the company considers, along with an analysis of the dates, nature and other details pertaining to the source:

Income:

- Recent Payslips (for the last 3 months);
- Employment Contract;
- Income Tax Records;
- Signed letter of engagement or employment contract confirming compensation;
- Bank Statement highlighting salary and/or other income.

Investment Proceeds:

- Document showing the initial investment proceeds which had been legally obtained;
- Document showing the investor owned the investment and receipts showing the sale of the investment proceeds.

Sale of Property:

- Document showing the purchase contract of the property;
- Document showing the title of the property showing ownership tax receipts paid on the property.

Ownership in a company / Company Sale or Sale of an interest in company:

- Signed letter from solicitor / letter from regulated accountant of sale and sight of investment monies on bank statements;
- Copy of contract of sale and sight of investment monies on bank statements;

- Letter from the financial authorities showing ownership of companies or directorship of companies.

Gift / Inheritance:

- Grant of Probate (with a copy of the will) which must include the value of the estate/property or Solicitor's letter;
- Letter from donor confirming details of gift (amount, date given and reason) and acknowledging the source of the donated funds.

Compensation Payment:

- Letter or court order from compensating body or a solicitor's / Advocate's letter showing amount, date received and information as to where the source of these funds has been derived from.

Gaming Winnings:

- Letter from relevant organisation on their letter-headed paper (lottery headquarters/betting shop/casino), stating the applicant's full name and residential address, date of win and amount won;
- Bank statements showing funds deposited by the named organisation;
- Copies of any media coverage would help as supporting evidence.

Cryptocurrency:

- Profit and loss statement on trading;
- Proof of settlement into the player's payment method.

When during an ongoing monitoring we come across high-risk situations and request SoF documents from a customer, we also have to re-assess the risk profile and all other relevant facts pertaining to that customer profile.

Moreover, in situations presenting higher risk of ML/TF/PF, SoF is to be requested from time to time even though there may not be any changes in pattern or activity conducted by the customer. Thus, for instance where the amounts deposited by a customer are particularly large, even if these amounts may be in line with the customer profile, we are still obliged to carry out enhanced ongoing monitoring to meet our obligations at Law. This includes obtaining information and documentation on the SoW and source funds used by the customer to fund the particularly large transactions.

7.3 Enhanced Due Diligence and Enhanced Ongoing Monitoring

Enhanced Due Diligence ("EDD") is to be applied whenever the Company identifies any high-risk situations. EDD entails taking more stringent steps in the application of CDD as well as requesting more detailed information on SoW and SoF.

It is important to mention that there are certain types of customers and certain situations (refer also to the Section 6.4) which are deemed to be high risk, independently of the risk assessment results, when the application of EDD measures is required as soon as reasonably possible and irrespectively of whether a 2000 Euro transaction threshold has been reached or not.

Mandatory High-Risk Situations that require Enhanced Due Diligence are the following:

1. PEP customers, their family members or their close associates (for the Compliance Officer to consider that such individuals could be accepted as our customers);
2. Customers from High-Risk and Non-Reputable Jurisdictions (FATF list);
3. In situations when we develop a suspicion or have reasonable grounds to suspect that activity in the account or a customer is linked to ML/TF/PF;
4. In cases where we discover that a customer has provided false or stolen identification documentation or information and the company proposes to continue to deal with the customer;
5. In cases when there are questions on the funding method being used by the customer, or when there are doubts as to whether the payment method used actually belongs to the customer;
6. In any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or a transaction or transactions have no apparent economic or legal purpose;
7. In any other high-risk situations determined by the Company from time to time, taking into account current trends.

The EDD measures include:

1. All standard CDD measures, described above in the Section 7.2, including documentary evidence of SoW/SoF;
2. Obtaining additional information on the customer:
 - a. obtaining a copy of the second form of identification to collaborate details;
 - b. obtaining a photo of an ID document held next to the player's face;
 - c. verification of the payment methods used for transactions in the account.
3. Taking additional measures to understand better the background, ownership and financial situation of the customer:
 - a. Open-source intelligence – Instagram, Facebook and other social media platforms to build the customer's profile, including looking at available photos online regarding customer's occupation, hobbies and activities.
 - b. Internet search on the customer's name, email address and phone number. The information could be useful to see whether the customer's name is linked to another person's identity or to some negative publicity, illegal activities etc.
 - c. Google Map search – in order to check the address, registered in the account and evaluate the financial situation of the customer.
4. Where the risk is not High, a Declaration on Source of Wealth/Funds (as attached in **Appendix 2**) may suffice, on a case-by-case basis;
5. Analysis of the interaction with the customer:
 - a. General chats with the customer;
 - b. Responsible Gambling interactions including calls;
 - c. Explanation for mismatches or inconsistencies in the account;
 - d. Timing of responses and co-operation.
6. Increasing the monitoring of the business relationship (**enhanced ongoing monitoring**), including greater scrutiny of the transactions.

8. APPLICATION of the CUSTOMER DUE DILIGENCE MEASURES

8.1 Application and Timing of CDD / EDD Measures

Based on the described above approach, the Company shall duly apply CDD measures in the following cases:

1. when establishing a Business Relationship (PEP/Sanction check);
2. when there is a suspicion of ML/TF/PF, regardless of the amount of the transaction;
3. when there are doubts about the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification;
4. when a customer reaches the €2,000 transaction threshold regardless if the threshold was reached in a single transaction or in several linked transactions and whether on the same or multiple brands;
5. when a customer reaches certain deposit thresholds;
6. at other appropriate times to existing customers on a risk-based approach;
7. when we become aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed;
8. any other event when the Compliance Officer finds it necessary.

While carrying out the CDD measures, customers may be allowed to continue using their gaming accounts while the Company obtains any necessary information from the customer concerned.

However, until such time as we obtain the necessary information and documentation from the customer to meet our CDD obligations, the customer **is not to be allowed to effect any deposit or withdrawals from the account independently of the amount involved.**

Our Terms and Conditions state that a customer has to provide all documents and other evidence requested by us to complete our checks within thirty (30) days of the date of our request. Such requests may be sent in the following scenarios (but not limited):

1. **2000 Euro transaction threshold reached (and account is not verified)** – an email is sent to a customer advising to submit documents. Customer is permitted to use the account normally, playing and betting activity is allowed, No Deposit / No Withdrawal restrictions apply. However, after thirty (30) days, the account is blocked manually if the customer doesn't provide the requested documents to the Company's satisfaction.
2. **Large Single Withdrawal or Multiple Withdrawals in a short amount of time and account is not verified (amount is 1000EUR or more)** – an email is sent to a customer advising to submit documents in order to approve withdrawal(s).
3. **High-Risk Customers/Situations** – “No Deposit / No Withdrawal” restrictions are applied before documents received. Once the thirty (30) day period lapses and no documents have been received, account is blocked.
4. When there are **some discrepancies** in the account or we can't “**close the loop**” when processing a withdrawal. Some payment methods are non-refundable, which means that we can't return winnings to the same account as was used by a customer to deposit. In such

situations we need to verify the ownership of payment methods before processing a withdrawal.

8.2 Inability to Complete CDD Measures

In the case of inability to complete or apply the required CDD measures in relation to a particular customer at any point or at the point the CDD threshold for transactions has been reached, even though we may have repeatedly asked a customer to forward said information or documentation, after **the lapse of thirty (30) days from the initial request we:**

1. will terminate the business relationship with the customer – the account will be blocked, meaning no activity will be allowed for a customer;
2. will inform the customer about our decision by email.

In the event when a customer makes the requested information and/or documentation available to us following the blocking of the gaming account, the account may be reopened, provided that CDD measures are completed.

The AML team with the assistance of the Compliance Officer will consider if the reluctance of the customer to provide CDD documentation affects the risk of ML/TF/PF associated with this particular customer. However, in such instances we need to consider all factors and information, including deposit/withdrawal patterns, payment methods used and any other information we hold.

In cases when there are grounds to suspect ML/TF/PF, the report will be submitted to the FIUs as soon as possible, and we will wait for the FIU's decision regarding the remaining funds.

In the event the Company is unable to remit the funds to the same source through the same channels, we will inevitably have to request fresh instructions from the customer. In the event that these instructions give rise to a suspicion we are required to submit a STR and suspend the remittance pending the FIU expressing its opposition or otherwise to the said transaction.

8.3 Termination of Business Relationship

In order to mitigate the ML/TF/PF Risks and to avoid potentially committing one of the principal money laundering offences, the Company shall terminate the business relationship with a customer in the following non-exhaustive list of circumstances:

- where it is known that the customer is attempting to use the company to launder criminal proceeds or for criminal spend;
- where the risk of breaches to AML Law and Regulations are considered by the Company to be too high, including customer's unusual transactions reported internally according to **"Internal and External Reporting Procedure"**;
- where the customer's gambling activity leads to an increasing level of suspicion, or actual knowledge, of criminal activity, including but not limited to money laundering;
- where the customer is proven to a reasonable degree of confidence to have an identity which is different to the one for which documents have been provided;

- where we suspect the customer of using stolen, cloned or otherwise unauthorised credit or debit cards;
- where we suspect the customer of using unfair advantage or influence (commonly known as cheating), including the exploitation of a fault, loophole or error in our software, the use of automated players or other devices or software, such as robots, that distort normal games play.

Additionally, where, in relation to any customer, the Company is unable to apply CDD measures, the business relationship with the customer must be terminated and the Compliance Officer must submit a SAR to the FIUs where they consider the circumstances to be suspicious.

9. FUNDS MANAGEMENT

The Company tries to mitigate the risk of ML/TF/PF by only using payment methods that are licenced by financial institutions. The Company will stop using a payment method should an authority (e.g., Curacao Gaming Control Board) explicitly instruct the Company to refrain from using such a method. In addition, the Company will never allow players to either deposit or withdraw in cash. All funds deposited by the player will be credited to the player's corresponding back-office account.

Additionally, in order to mitigate ML/TF/PF risks, where possible, upon a withdrawal request, the Company shall use a "closed loop policy" and thus the Company will only remit withdrawals to the same account from which the funds originated.

There could be payment methods that do not allow the Company to apply the "closed loop policy". In such cases, the customer will be asked to provide proof of ownership of both the deposit and the withdrawal methods within thirty (30) days from the date of the request. The player's account will be closed should the player not submit the necessary documentation on time and the Compliance Officer will assess whether a SAR/STR report needs to be submitted to the FIU.

10. REPORTING SUSPICIOUS ACTIVITY and TRANSACTIONS

The Company understands that Suspicious Transactions and Activity Reporting has to be considered as the most important AML/CFT obligation of all, and the Company is fully committed to ensure that any suspicious transactions and activity are brought to the FIU's attention without delay.

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

Relevant employees will receive training in how to make an internal Suspicious Activity Report.

10.1 Unusual Transaction Reporting

The definition of a suspicious activity and transaction as well as the types of transactions indicating ML/TF/PF is very broad. A suspicious transaction will often be inconsistent with the normal Business

Relationship patterns of the specific account. The Company shall ensure that it maintains adequate information and knows enough about its customers' activities in order to recognize on time that an activity, a transaction or a series of transactions are unusual or suspicious.

Examples of what might constitute suspicious transactions/activities related to ML/TF/PF are listed in **Appendix 1** of the AML/CTF/CPF Policy. The relevant list is not exhaustive, nor does it include all types of activities or transactions that may be used. Nevertheless, it can assist and serve as guidance to the Company and its employees (especially the Compliance Officer and AML Team).

To comply with the Curaçao AML-regulation (The Decree Indicators Unusual Transactions [“Regeling Indicatoren Ongebruikelijke Transacties (PB 2015, no. 73), Annex F”]) the Company obliged to report all **complex or unusually large transactions** or all **unusual transactions** with no apparent economic or clear purpose.

A transaction (executed or proposed) is deemed to be unusual if one or more of the below indicators apply.

Objective indicators (indicators that based on knowledge or facts and not open to interpretation):

1. A transaction that is reported to the police or the judicial authorities in connection with money laundering or the financing of terrorism.
2. A proposed transaction by or for the benefit of a natural person, whose name appears on a list that has been drawn up pursuant to the Sanctions National Ordinance.
3. A transaction of the value of two thousand Euro (€2,500) or more:
 - Deposit transaction (regardless of the payment method used)
 - Pay-out transaction

Subjective indicators (indicators that are based on suspicion or previous experience):

- Transactions that give reason to assume they could be related to money laundering or to the financing of terrorism.

10.2 Internal Reporting Procedure

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

a. Knowledge

Having knowledge means actually **knowing something to be true**. In case the Compliance Officer or any other employee is aware or is in possession of information of ML/TF/PF activities, the Compliance Officer should immediately proceed with filing a report with the FIU.

b. Suspicion

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

c. Reasonable Grounds to Suspect

The requirement to file a report goes beyond “suspicion” and also includes the obligation to report when “reasonable grounds to suspect” exist. This implies that a further obligation to report arises where, on the basis of objective facts or circumstances, a reasonable person would have inferred knowledge or formed the suspicion that ML/TF/PF existed or that funds were the proceeds of criminal activity.

The Compliance Officer is responsible to ensure that all of the Company’s employees:

- are aware of the Internal Reporting Procedure;
- understand its importance and the consequences of their failure to report;
- understand that reporting is a legal defense against prosecution;
- know, where to find an Internal Suspicious Activity Report template and other supporting information and
- know how to avoid a “Tipping Off” offence.

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

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

Internal reports are to be submitted in writing by using a special template document titled **“Suspicious Activity Report” (Appendix 3)** and advised to include as much details as possible.

All internal suspicions reported to the Compliance Officer, all internal enquiries made in relation to the report will be electronically documented.

10.3 Internal Evaluation and External Reporting

It is the responsibility of the Compliance Officer to receive and evaluate all Internal SAR/STR and report to the appropriate FIU any transaction or activity where, after their evaluation, they know or suspect, or have reasonable grounds to know or suspect, may be linked to ML/TF/PF. Such reports must be treated with the utmost urgency and submitted to the FIU **on the same day** when knowledge or suspicion of ML/TF/PF is considered to subsist by the Compliance Officer.

In a complex case, when a lot of information and documentation has to be prepared and submitted, and the submission of the SAR/STR is not possible within the same day, the Compliance Officer shall ensure that the Report is filed within the shortest time possible.

The decision to file or not to file an STR/SAR must **always be the Compliance Officer’s own**, and should not be subject to the direction or approval of senior management of the Company.

In order that an informed overview of the situation may be maintained, all contact between the company and the FIU should be controlled through, or reported back to, the Compliance Officer or a designated employee, acting as a deputy in the absence of the Compliance Officer.

The External Reporting will be submitted via **GoAML Portal** and in order to submit external SAR/STR, the Compliance Officer must be registered with the FIU and have logins to the GoAML Portal.

The detailed description of the reporting process is to be found in **“Internal and External Reporting Procedure”** document, including but not limited to

- the time scale and way of reporting;
- what is the “requesting a defence / consent” process;
- record keeping process;
- the template of the Internal Suspicious Activity Report and the explanation on how to fill it in;
- the information about the different types of External Reports and what to include in it;
- the time scale for the FIU to respond;
- actions after reporting;
- Prohibited and Permissible Disclosures;
- Licence specific reporting requirements.

10.4 Prohibited and Permissible Disclosures

By Law we are prohibited from disclosing to the person concerned or to the third party that:

1. An STR/SAR has been made to the FIU;
2. The FIU has requested information within the context of an ML/TF/PF analysis;
3. Information has been given to the FIU within the context of an ML/TF/PF analysis;
4. An ML/TF/PF analysis or investigation has been, is being or may be carried out by the FIU or by any other competent law enforcement agency.

The term ‘third party’ includes any person who is not an employee of the company (including outsourcing).

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

However, the Company is permitted to disclose the above-mentioned information to our supervisory authority as well as to law enforcement agencies.

11. RECORD KEEPING PROCEDURES

The Company must retain records of any business relationship it enters into and of any transaction it carries out. These records are to include any documentation and information produced or obtained in complying with our obligations under the AML Law and Regulations, as well as under LCCP and other guidance issued by the supervisory authorities.

The main purpose of keeping records is:

1. Show our compliance with the obligations at Law;
2. Assist the Company in revising its AML/CFT Policies and Procedures, especially in revising its Business Risk Assessment;
3. Ensure effective ongoing monitoring;
4. Assist the FIU, relevant supervisory authorities and law enforcement agencies in the prevention, detection, analysis or investigation of possible ML/TF/PF.

11.1 Records to Be Retained and Retention Period

The Company shall maintain records of all documents related to the verification process performed on a customer in relation to all business relationships formed:

- the player identification documents obtained during the CDD/EDD, as applicable;
- PEP / Sanctions Reports received;
- monitoring reports obtained during and after the establishment of Business Relationship as well comments from CS agents or AML team and other communication with the player;
- transaction history including amount, currency, time and payment methods.

The Company should also retain the following records required as evidence of compliance with AML regulations:

- internal SARs made to the Compliance Officer;
- external SARs, including decisions and actions taken by the Compliance Officer;
- a record of the reasons for not forwarding an internal report to the FIU Curacao;
- contact between the Compliance Officer and law enforcement or the FIU Curacao;
- a record of AML/CTF/CPF training provided, including: the date on which the training was delivered; the nature of the training; the names of employees receiving the training; the results of any assessment undertaken by employees; a copy of any hand-outs or slides;
- any reports by the Compliance Officer to senior management made for the purposes of complying with the obligations under the Law;
- Copies of Approved AML/CFT/CPF Policies and Procedures;
- Record of Business Risk Assessment, Technological Risk Assessment and Customer Risk Assessment.

The Company must maintain the records, specified above, normally for a period of five (5) years. However, in some cases the FIU, the supervisory authorities or law enforcement agencies have the right to demand those records be retained for a longer period when this extension is considered necessary for the purposes of the prevention, detection, analysis and investigation of ML/TF/PF activities by the FIU Curacao or law enforcement agencies.

Upon expiry of the five-year retention period, any personal data must be deleted unless:

- the Company is required by the relevant supervisory authorities, FIU or law enforcement agencies that records, including personal data, be retained for longer periods, when this

extension is considered necessary for the purposes of the prevention, detection, analysis and investigation of ML/TF/PF activities;

- the subject of the data has agreed to the retention of the data, or
- the Company has reasonable grounds for believing that records containing the personal data need to be retained for the purposes of legal proceedings.

However, the company cannot be directed to hold any records indefinitely since the retention period **as extended** can never exceed **ten (10) years in total**.

11.2 Retrieval of Records

The Company will ensure that there is an effective system in place that enables it to respond efficiently, adequately, promptly and comprehensively to the enquiries made to the Company by the FIU, supervisory authorities or law enforcement agencies in accordance with applicable law.

When requests for information are made by the financial intelligence unit, we should ensure that we are able to reply to these enquiries in a timely manner, but not later than **five (5) working days** from when the demand is made. It should be noted that the FIU may impose a shorter response time for replies to requests for information.

The retrieval system has to enable us to respond efficiently, adequately, promptly and comprehensively to such inquiries.

To facilitate the retrieval of records and to assist in any compliance monitoring activity conducted by the FIU or other relevant supervisory authorities, the Company to maintain a list of our current business relationships setting out at the minimum:

- the name of the customer and/or customer reference number;
- the risk categorisation of the business relationship (risk rating or risk score);
- the type of products used;
- the date of commencement of the business relationship and, where applicable, the date on which it ceased;
- country of residency of a customer;
- whether the customer is a PEP, an immediate family member or a close associate of a PEP;
- Self-Exclusion status and details of the Self-Exclusion period;
- whether reliance has been exercised with respect to the particular business relationship.

APPENDIX 1. RED FLAGS

There are certain red flags we need to be aware of, which on their own would not constitute conclusive proof that a customer is involved in money laundering activities. We need to evaluate the situation, the customer profile and the account taking into consideration everything we know and can find out about the customer.

The non-exhaustive list of examples of suspicious activities and transactions that can raise the suspicion of Money Laundering or Terrorist Financing is the following:

1. Amount and Volume of Transactions

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

2. Deposit / Withdrawal

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

- A customer makes frequent deposits and withdrawal requests without any reasonable explanation.

3. Verification / Communication

- A customer is reluctant to provide complete information when establishing a Business Relationship.
- A customer provides unusual or suspicious identification documents that cannot be readily verified.
- A customer's registered details seem to be incomplete or incorrect.
- Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g., previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).
- Unwillingness to interact or communicate.
- A customer is asking a lot of questions about KYC and Verification Procedure, PEP Policy or AML Policy.
- Customers who end the relationship because they are required to provide information. Customers who resist or refuse to provide information.
- Customers who provide the same address or telephone number as another customer, with whom they do not appear to have a connection.

4. Betting / Playing Behaviour

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

5. Account Re-activation

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

6. Customers' profile

- Activity not justified on the basis of a customer's source of wealth or not keeping with the average profile.
- There is negative publicity implicating the customer with crime, terrorism or organisations linked to terrorism.
- The customer has links to a jurisdiction or area where terrorists are active or which are known to sympathise or support terrorists or terrorist organisations.
- Transactions in which payments are made with funds originating in tax havens, countries or territories that do not cooperate in the fight against money laundering and terrorist financing, or in states where there is knowledge of the existence of particularly active criminal organizations.
- Customers where there are indications that they act on behalf of others, seeking to hide the identity of the actual customer.
- Customers who have the status of or are related to politically exposed persons (i.e., persons who perform or have performed significant public functions in another country).
- Customers with published police or criminal records or linked to persons prohibited from trading or to terrorist financing activities.
- Customers attempt to register more than one account with us.

APPENDIX 2. SOURCE of WEALTH/FUNDS DECLARATION

SOURCE OF WEALTH DECLARATION FORM

Full Name: _____

I hereby declare that the funds I use to deposit into my InterStorm account are derived from legitimate earnings.

My main source of income is _____, from which in the past year, I've earned _____, and on average I earn circa _____ per month from this activity.

Please find attached proof of income from the main source of income.

My secondary source of income is _____, from which in the past year, I've earned _____, and on average I earn circa _____ per month from this activity.

Please find attached proof of income from the secondary source of income.

I hereby declare that the above information, and the attachments are accurate and complete.

Signature:

Date:

APPENDIX 3 – INTERNAL SAR/STR TEMPLATE

<u>Internal SAR</u>	
<u>Current Date:</u>	
<u>Player ID/Username:</u>	
<u>Nickname:</u>	
<u>Email / Status:</u>	
<u>Phone / Status:</u>	
<u>Gender:</u>	
<u>First Name:</u>	
<u>Last Name:</u>	
<u>Address:</u>	
<u>Last Login Date:</u>	
<u>Registration Date:</u>	
<u>CDD/EDD:</u>	
<u>Occupation provided:</u>	
<u>Account status:</u>	
<u>Documents Provided:</u>	
<u>Account balance:</u>	

Please provide a detailed explanation of the suspicious activity or transaction that occurred below including the reasoning as to why it is grounds for knowledge and/or suspicion.

-