

High Gaming IT Services BV

POLICY

for Prevention and Combatting of Money Laundering and Terrorist
Financing

VERSION CONTROL

Version	Version Date	Approved By
1.0	2024-07-01	Ying Ma, CEO

ABBREVIATIONS

AML, TF & FP	Anti-money laundering, prevention of the terrorist financing & financing of proliferation
BO	Beneficial Owner
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFATF	Caribbean Financial Action Task Force
CFO	Chief Financial Officer
CO	Compliance Officer
CRA	Customer Risk Assessment
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know your customer
MLRO	Money Laundering Reporting Officer
NOIS	National Ordinance on Identification of clients when Rendering Services
NOPML	National Ordinance Penalization of Money Laundering Regulations
NORUT	the National Ordinance on the Reporting of Unusual Transactions
NRA	National Risk Assessment
PEP	Politically Exposed Person
RBA	Risk Based Approach
Regulations	
Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction	
SDD	Simplified Due Diligence
SoF	Source of Funds
SoW	Source of Wealth
STR	Suspicious Transaction Report
The Policy	the Policy on Prevention of Money Laundering and Terrorist Financing
UBO	Ultimate Beneficial Owner
UTR	Unusual Transaction Report

1. POLICY STATEMENT

The management of (the “Company”) is committed to combat the abuse of the Company’s services for the purpose of ML, TF, FP. In light hereof the Company is committed to comply with the applicable legislations, in particular regarding the identification of clients and the reporting of unusual transactions.

To facilitate compliance the Company has implemented a risk based compliance program consisting of the following pillars:

1. Establishing policies, procedures and internal controls designed to prevent the business from being used to facilitate ML or other criminal activities and to ensure compliance with applicable reporting requirements.
2. Appointment of a senior CO/MLRO having sufficient knowledge, authority and resources to oversee the Company’s AML program;
3. Employee screening program and ongoing employee training program;
4. A system of independent testing of the AML/CFT/CFP policies and procedures in place to ensure their effectiveness.

2. PURPOSE & LEGAL FRAMEWORK

The Policy outlines the general unified standards and procedures of AML, TF & FP which must be adhered to by the Company, its directors, officers and employees.

This policy is based on the following legal provisions:

- The NOIS (N.G. 2017, no. 92);
- The NORUT (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the NORUT
- (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations’ Security
- Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations’ Security
- Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions
- Decree People’s Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

3. AUDIENCE

This policy applies to all activities, services, products, and Employees of the Company, including the Company's officers, directors, full-time Employees, part-time Employees, temporary Employees, or contractors employed by the Company or affiliates of the Company, as well as the Company's third-party service providers as relevant. Such individuals will be provided with regular training to ensure awareness of this policy and their obligations under it, at least on an annual basis or more frequently as required. All employees are also expected to familiarize themselves with the third-party vendors engaged by the Company to assist in AML activities related to fiat currency and crypto currency. The Company processes transactions in crypto currency, and intends to process transactions via credit card and other forms of fiat currency; to these endeavors, the Policy and Program is intended to address the scope and breadth of all such transactions and ensure that the Company does not engage, foster, aid, or otherwise encounter any forms of illicit money laundering or terrorism financing.

4. DEFINITION OF ML, TF & FP

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three phases.

Cash first enters the financial system at the "placement" stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Broadly, the international AML, TF & FP provisions are aimed at requiring firms to:

- identify customers and suspicious transactions at the placement and layering stages
- keep adequate records which should prevent the integration stage being reached, and also provide an audit trail for investigators, and
- report suspicious activity or behavior to the relevant regulatory or legislative authority.

Terrorist financing may not always involve funds derived from criminal activities; instead, it often seeks to hide the origin or intended use of funds, which could be for illicit purposes. The primary distinction between terrorist financing and money laundering lies in the source of the funds. Unlike traditional criminal organizations, terrorist financiers may rely on legitimate sources of funding. These sources can include charitable donations, foreign government support, business ownership, and personal employment. Despite differing motivations, the methods used to finance terrorism can be similar to those employed by criminals to launder money. Terrorist operations may not require large sums, as funding can be accumulated over time, with transactions that are relatively simple and not immediately suspicious.

FP is the provision of funds for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions require countries to freeze funds and assets, ensuring that no funds or assets are made available, directly or indirectly, to designated persons or entities. In Curaçao, all individuals and legal entities must promptly and without prior notice freeze the funds or assets of designated persons and entities. This obligation aligns with United Nations Security Council resolutions and the European Union's Common Foreign and Security Policy. Compliance with UN Security Council sanctions is mandatory under the United Nations Charter, while EU sanctions are binding on Curaçao through the Kingdom Sanctions Act.

Mechanisms must be in place to verify the sanction status of withdrawing participants to prevent sanctioned individuals or organizations from accessing funds that should be frozen.

5. POLICY IMPLEMENTATION

The Company will follow applicable directives issued in conjunction with the necessary regulatory bodies to prevent ML, TF, FP, sanction violations, and other criminal activity. The Company will not engage in activities related to these activities or involving any person or business who is under US, UN, or EU sanctions or a partner's prohibited countries or watchlists or involving any country or region subject to comprehensive US sanctions.

The Company has a four-stage risk-based approach to combatting ML, TF, FP sanctions violations, and other criminal activity:

- A. Identification: Identifying the Company's products and services could be used for money laundering and/or terrorist financing;
- B. Documentation: Ensuring that the Company has clear and well documented policies and procedures in place for employees to understand the risks, to know what to look for, and to know how to report any unusual activity;
- C. Mitigation: Implementing strong measures and defense mechanisms to prevent money laundering, terrorist financing, and other criminal activity from occurring in the first place or enabling the Company to detect and report such occurrences if they do happen; and
- D. Monitoring: Closely monitoring identified risks and mitigating them by using the established measures on an ongoing basis and, where necessary, adjusting to any changes.

5.1 RISK BASED APPROACH

Based on the FATF Recommendations, gaming companies are required to apply a Risk-based Approach to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified.

Applying Risk-based Approach means that the Company:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- 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;
- Document their risk assessments, including everything that has been done and the reason for this being done.

Given that risks are dynamic, the Company subscribes to continuously monitor the effectiveness of these policies, procedures, and controls, making necessary adjustments as needed. The risk assessment must also be made available to the CGA upon request.

5.1.1. BUSINESS RISK ASSESSMENT

The Company conducts a comprehensive Business Risk Assessment (BRA) to identify and evaluate its exposure to ML, TF, FP and sanctions risks. The assessment ensures that AML/CFT controls are commensurate with the risks associated with the Company's operations, products, services, customer base, and geographical footprint.

The BRA is reviewed annually and upon any material change to business operations or regulatory obligations. The BRA includes the following key areas:

Product and Service Risk: Evaluation of the ML/TF risks inherent in the Company's gaming offerings (e.g., online poker, sports betting, and virtual currency). Particular focus is placed on features allowing for rapid fund movement or cashout without proportional gameplay.

Customer Risk: Classification of customers by risk levels based on geographic origin, payment behavior, funding methods, and whether they are high-net-worth individuals, Politically Exposed Persons (PEPs), or associated with high-risk industries.

Geographic Risk: Analysis of exposure to countries listed by FATF, OFAC, or other relevant authorities as non-cooperative or high-risk, as well as jurisdictions with weak AML/CFT systems or under international sanctions.

Transactional Behavior Risk: Detection of patterns such as minimal gaming activity before large withdrawals, unusual use of bonuses, or frequent account top-ups followed by inactivity.

Findings from the BRA are documented and used to inform risk-based procedures and customer due diligence protocols. The effectiveness of controls derived from this assessment is validated through internal audits, transaction monitoring results, and independent testing.

5.1.2. CUSTOMER RISK ASSESSMENT

The Customer Risk Assessment (CRA) is an essential element of the Company's risk-based approach, aimed at evaluating the ML/TF risk posed by individual customers. It informs the level of due diligence, ongoing monitoring, and other controls applied to each customer.

Each customer is assigned a risk rating (Low, Medium, High, or Very High) based on a set of risk indicators:

Identification and Verification Data: Including full name, address, date of birth, and documentary or non-documentary verification.

Behavioral Factors: Transaction volumes, frequency of deposits and withdrawals, and patterns of gameplay versus monetary activity.

Geographic Indicators: Whether the customer is based in or connected to high-risk or sanctioned jurisdictions.

Payment and Funding Sources: Use of crypto-assets, pre-paid cards, or anonymous funding methods increase risk; documented employment income or regulated bank transfers lower risk.

Third-party Data: Alerts or insights from vendors (sanctions and PEP screening, blockchain transaction tracing).

CRA is initiated at account creation and continuously updated based on the customer's activity and external inputs. Triggers for re-evaluation include:

- Cumulative deposits exceeding defined thresholds (e.g., \$2,000 or Cg. 4,000, whichever is less).
- Document KYC Verification.
- Attempted withdrawals or redemptions.
- Alerts from internal or third-party systems.

High-risk customers undergo Enhanced Due Diligence (EDD), including documentation on source of wealth and intended usage of the platform.

The CRA informs decisions on whether to escalate accounts, impose restrictions, or file unusual transactions to the FIU.

5.2. CUSTOMER ACCEPTANCE POLICY

The Customer Acceptance Policy (CAP) sets forth the onboarding requirements and thresholds for escalating due diligence procedures based on CRA outcomes. The Company uses a three tiered Customer Identification and Verification system:

Level 1: Account Creation Required: Email address. Purpose: Establish account credentials and provide CIP notification. Limitations: No monetary transactions permitted.

Level 2: Customer Due Diligence (CDD) Triggered by: First attempted deposit or wager. Required Information:

- First and Last Name
- Phone Number
- Full Residential Address (no P.O. Boxes; APO/FPO acceptable)
- Date of Birth
- Government-issued ID Verification (subject to specific policies and management's discretion); The user-provided information must be verifiable by third-party vendors (including Sardine A.I. and Chainalysis) prior to transacting above the prescribed limits and can be provided in two ways: either as photos of government issues, unexpired IDs/selfie uploads (documentary), or as text inputs (non-documentary) when made available.

Level 3: Enhanced Due Diligence (EDD) Triggered by:

- Withdrawal attempts or redemptions
 - Cumulative deposits exceeding \$2,000 or (Cg. 4,000, whichever is less)
 - Behavioral red flags or vendor alerts
 - Additional Requirements:
 - Documentary proof of address (e.g., utility bill or bank statement)
 - Source of wealth/income documentation for high-risk accounts, if applicable
 - Explanation of transactional behavior or relationships, if applicable
- All KYC information must be verifiable via approved third-party providers before the customer is allowed to transact beyond set limits

Restricted Jurisdictions

The Company prohibits customers from countries under comprehensive sanctions and on the FATF's High-Risk Jurisdictions subject to a Call for Action list (e.g., Iran, North Korea, Syria, Myanmar) and maintains:

- A Non-Supported Countries List
- A Prohibited Jurisdictions List for monitoring and reference

Account Escalation and Review

High-risk accounts are subject to Compliance approval.

Customers that are classified as PEP are per default considered high risk customers. PEPs are subject to management approval.

The term "Politically Exposed Persons" is broad and generally includes all persons who fulfill a prominent public function. This includes:

- i. Heads of State, Heads of Government, Ministers, Deputy and Assistant Ministers, and Parliamentary Secretaries;
- ii. Members of Parliament;
- iii. Members of the Courts of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- iv. Members of courts of auditors, Audit Committees or of the boards of central banks;
- v. Ambassadors, charge d'affaires and other high-ranking officers in the armed forces; and
- vi. Members of the administration, management or boards of State-owned corporations.

The term "immediate family members" of PEPs includes:

- i. The spouse, or any partner recognized by national law as equivalent to the spouse;
- ii. The children and their spouses or partners; and
- iii. The parents.

Sanctions screening

The Company is committed to complying with all applicable sanctions, including U.S. UN, and EU sanctions

Document Retention

All customer information and due diligence records are maintained for at least seven years from the date of collection or account closure, whichever is later.

5.3 CUSTOMER DUE DILIGENCE

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. It must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions. A sound CDD program is the best way to prevent AML, TF & FP.

The customer's risk profile is essential to apply a certain level of CDD commensurate to the identified ML/TF risk. The purpose of collecting information is to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behavior, which are reported to the FIU.

The obligation to undertake CDD measures when:

- When players engage in financial transactions equal to or above Cg 4,000 or equivalent EUR 2,000;
- carrying out occasional transactions above the monetary equivalent of EUR 2,000;
- there is a suspicion of money laundering or terrorist financing; or
- there are doubts about the veracity or adequacy of previously obtained customer identification data.

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of EUR 2,000.

For transaction above the monetary equivalent of EUR 2,000, CDD measures are applied immediately. Whether the transaction is carried out in a single operation or in several operations which appear to be linked. Transactions are considered as linked if they are carried out by the same customer through the same game or in one gaming session. A transaction consists of the wagering of a stake or the collection of winnings.

The CDD measures to be taken are as follows:

- a. Identifying the player documents, data or information;
- b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions

undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, its source of funds.

5.3.1 IDENTIFICATION AND VERIFICATION OF THE PLAYER

Identification refers to the collection of personal details of the player to establish the identity of the player. Verification, on the other hand, consists of confirming the personal details collected for identification purposes using reliable, independent source documents, data or information. The personal information required and extent of verification to be carried out, will vary depending on risk of the customer.

When identifying the player, at a minimum the following information must be collected:

- i. full name;
- ii. permanent residential address;
- iii. date of birth;
- iv. place of birth;
- v. nationality; and
- vi. identity number.

However, in low risk scenarios a limited identification to the three personal details set out in (i) to (iii) above. On the other hand, in high risk situations, it is possible to collect additional personal details as necessary to mitigate the higher risk of ML/FT.

5.4 ONGOING MONITORING

The Company will conduct ongoing monitoring to identify concerning transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for concerning transaction reporting.

The Company will utilize a combination of automated and manual monitoring methods applying internal tools, the vendor reports, and referrals from Partners (card networks, financial institutions, etc.).

By monitoring transactional activity through the combined use of technology and manual analysis. The objectives of an effective transaction monitoring process include:

- A. A risk-based monitoring methodology;
- B. A proficient review process;
- C. A competent escalation process; and
- D. The prompt reporting of unusual activity.

The Compliance department will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, and will document when and how this monitoring is carried out.

5.5 RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE

The Company may, under specific circumstances, rely on third parties to perform certain elements of the Customer Due Diligence (CDD) process, provided that the following conditions are met:

A. Permitted Activities for Third Parties

Third parties may be relied upon to:

- Obtain identification and verification information of the customer and, where applicable, the beneficial owner;
- Verify the identity of the customer and beneficial owner;
- Understand the nature and intended purpose of the business relationship.

B. Third-Party Qualification and Risk Assessment

Before engaging a third party for CDD purposes, the Company shall ensure:

- The third party is a regulated financial institution, gaming operator, or another person or entity subject to equivalent AML/CFT regulations;
- The third party has robust internal AML controls and procedures;
- A documented risk assessment of the third party has been completed;
- A contractual agreement is in place that obligates the third party to comply with applicable CDD requirements.

C. Access to CDD Data and Documentation

The Company must immediately obtain from the third party:

- All relevant CDD documentation, including identification and verification data;
- All records of the nature and intended purpose of the business relationship;
- Any ongoing monitoring data, as applicable.

Such documentation must be accessible by the Company at the time of reliance and available for regulatory inspection upon request.

D. Liability and Responsibility

The Company retains ultimate responsibility for compliance with all CDD obligations, including the actions of any third party it relies upon. Reliance on third parties does not exempt the Company from ensuring the completeness, accuracy, and timeliness of CDD measures.

E. Ongoing Monitoring of Third Parties

The Company will:

- Periodically review third-party relationships to ensure continued compliance with contractual obligations and applicable AML/CFT laws;
- Terminate relationships with third parties who fail to meet expected standards;
- Maintain a log of all customers onboarded or verified via third-party providers.

5.6 REPORTING OF UNUSUAL TRANSACTIONS

The Company will report any unusual transactions to the Curacao FIU if they're believed to be involved in potential money laundering. To protect the Compliance department, the AML Compliance Person ensures The Company personnel can report violations of the Program anonymously. Employees engaging with customers or accessing customer information will receive anti-money laundering (AML) training to recognize unusual or potentially suspicious behaviors. If employees suspect involvement with proceeds of crime, they must submit an Internal Unusual Activity Report (IUAR) to the AML Compliance Person within 24 hours. The AML Compliance Person will investigate and determine if a report to the Financial Intelligence Unit (FIU) of Curaçao is warranted within 48 hours.

The Company staff will be trained to identify unusual transactions based on customer profiles and specific indicators. All unusual transactions must be reported to the CO in an approved format, accompanied by supporting documentation.

Unusual transactions include:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing of terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);

c. A transaction amounting to Cg. 5,000.00 or more (equivalent EUR 2,450), regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:

1. A cashless transaction in the amount of Cg. 5,000.00 or more.
2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
4. A cash out in the amount of Cg. 5,000.00 or more;

d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

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

The AML Compliance Person further ensures that this mechanism is well publicized to all personnel and will take necessary steps to ensure reports of potential violations remain anonymous and confidential. Regardless of whether a report is made anonymously, The Company has zero tolerance for retaliation against an employee for reporting a potential violation up to and including termination. All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

Further, the Company will retain copies of all actions, decisions, and processes outlined in this document for a minimum of seven years. The records will be electronically stored, to be printed as a hard copy when necessary. The records will also be organized in a manner that facilitates easy retrieval to enable reporting to the Curacao FIU without undue delay.

5.7 ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

The Company maintains proper internal controls to mitigate risks targeted by the Program with focus on customer identification and transaction monitoring. The Company has implemented the following internal controls to mitigate risks targeted by the Program: (i) KYC Program; (ii) Transaction Monitoring; (iii) Sanctions and Prohibited Jurisdictions; (iv) Fraud Prevention; (v) Employee training; (vi) Independent Testing.

- i. **Know Your Customer Program** – The Company has established, documented, and maintains a KYC Program. The Company will: (1) collect certain identification information from each customer; (2) utilize risk-based measures to verify the identity of each customer; (3) record customer identification information and the verification methods and results.
Each customer of the Company will be initially screened at onboarding and periodically thereafter for as long as they remain a customer.
- ii. **Transaction Monitoring** – is executed to prevent involvement of the Company with ML/TF and to safeguard the reputation of the Company. While in conducting ongoing scrutiny of transactions there are transactions that are not consistent with what it is expected from the customer, the Company establishes the source of the funds used for that transaction. The Company must obtain sufficient information and documentation with regard to the transaction to determine the reason for this deviation. If needed, the risk profile of the customer may have to be revised. After receiving this information, the Company decides whether the transaction is an unusual and needs to be reported to the FIU.

The level of on-going monitoring depends on the risk profile of the customer, but even in low-risk situations there is a degree of oversight to ensure that the business relationship is still considered as a low risk one.

The Company conducts ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the Company's knowledge of the customer, the customer's business and risk profile.

- iii. **Sanctions and Prohibited Jurisdictions** - The Company is committed to complying with all applicable sanctions, including U.S. UN, and EU sanctions, by taking the following measures:
 - a. prohibition of individuals or entities listed on applicable assets freeze lists, such as the US list of specially designated nationals and block persons, the EU consolidated list of financial sanctions targets, or any list maintained by any relevant authority;
 - b. prohibition of entities owned or controlled by entities on the lists referred above;
 - c. we prohibit and restrict Users in certain countries or territories. For example, US Persons are generally prohibited from dealing with Cuba, Iran, Syria, North Korea, and Crimea ("**Restricted Territories**")The Company will have in place a process to freeze and block accounts of all customers that are a confirmed sanctions match, and will escalate those customers to business partners requiring such escalations within 24 hours.

iv **Fraud Prevention** – the compliance program is focused to systemically detect, deter, and mitigate fraudulent activities. Involving a combination of policies, procedures, technology, and education to protect against fraud and related crimes.

v. Employee Training and Reporting Guide

It is required that all new employees subject to this policy, receive AML/OFAC training at least annually. New Employees are assigned to the training as a part of the onboarding process. Employees that are delinquent may be subject to disciplinary actions. Relevant employees include those responsible for the following:

- i. customer onboarding and due diligence (including high-risk customer monitoring;
- ii. monitoring customer transactions and electronic fund transfers;
- iii. addressing customer queries or concerns (customer service teams); and
- iv. technology functions related to AML activities.

The AML Compliance Person is responsible for developing a risk-based training program and ensuring that staff members requiring advanced training due to their job description and/or responsibilities within the Company receive such training. A training log will be maintained.

vi. Independent Testing

The Company will conduct independent testing on the Company's AML program on a periodic basis, and no less than twice annually. When conducted, the review will assess the implementation and effectiveness of the Company's AML/OFAC program and the adequacy of controls over any related risks. The Compliance Officer is responsible for updating the Company's risk assessment in regards to any issues raised during the independent testing and taking necessary corrective actions and remediate findings. Independent testing has not yet been conducted on the program but the decision to test will be determined at a later date.

6. COMPLIANCE & CONSEQUENCES OF NON-COMPLIANCE

Failure to comply with AML legislation may result in sanctions being brought against employees such as fines and imprisonment or the Company including criminal prosecutor, and/or fines. These could affect the Company's ability to operate as well as seriously damage the Company's reputation.

Separate and in addition to the foregoing, an employee may also be liable for failure to meet record keeping and client identification responsibilities and requirements, failure to provide assistance or provide information during a compliance examination, or disclosing the fact that a unusual transaction report was made, or disclosing the contents of such a report with the intent to prejudice a criminal investigation.

"Tip Off" shall be defined as revealing to a third party that an internal or FinCEN report has been filed. Similarly, **"prejudicing an investigation"** involves disclosing to a third party that law enforcement is either investigating or preparing to investigate an individual. Disclosing to a suspected money launderer that a disclosure has been made will almost certainly undermine any subsequent investigation,

"Assist"

An employee commits an offense if he or she: (i) enters an arrangement which he or she knows, or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person; (ii) acquires, uses or has possession of criminal property; and (iii) conceals, disguises, converts, transfers or removes criminal property.

7. RELATED INFORMATION

- A. KYC Policy Document (Know Your Customer) – Appendix.1
- B. Sanctions Compliance Policy – Appendix.2
- C. Internal Unusual Activity Report (IUAR) Form – Appendix.3
- D. AML/CFT Risk Assessment Template – Appendix.4
- E. AML Employee Training Manual – Appendix.5
- F. Customer Risk Assessment (CRA) Procedures – Appendix.6
- G. Transaction Monitoring Procedures – Appendix.7

8. CONTACT INFORMATION

For any questions regarding this policy, please contact:

Name: Ying Ma

Title: CEO

Email: leo.ma@betday.com

Phone: +55 11977181848

9. POLICY HISTORY

This is a **new policy**.

- **Version 1.0 – Effective Date: July 01, 2024**
Initial implementation of the Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Financing of Proliferation (FP) Policy.



Signed by e-Managment N.V. (Managing Director)

Transaction Monitoring Procedures

High Gaming IT Services BV

Effective Date: July 01, 2024

1. Purpose

These procedures define the systems and controls implemented by High Gaming IT Services BV to identify, analyze, and respond to suspicious or unusual transactions that may indicate money laundering, terrorist financing, fraud, or sanctions evasion. Transaction monitoring is a critical part of the Company's Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Program.

2. Monitoring Methods

The Company utilizes both **automated and manual** transaction monitoring techniques:

2.1 Automated Monitoring Tools

- Transaction monitoring software integrated with core platforms (e.g., Chainalysis, Sardine AI)
- Real-time rule-based alerting for:
 - Unusual deposit/withdrawal patterns
 - High-value or rapid transactions
 - Transactions involving flagged countries, currencies, or assets
- Blockchain analysis for crypto-related activities

2.2 Manual Monitoring

- Review by AML Analysts or Compliance Officer of flagged transactions
 - Case-by-case reviews of high-risk accounts or patterns
 - Manual audit of transaction logs and customer profiles
-

3. Risk-Based Thresholds for Review

Transaction activity is monitored against thresholds determined by customer risk ratings:

Customer Risk Level Trigger Thresholds for Review

Low	≥ \$2,000 (Cg. 4,000) per day
Medium	≥ \$1,000 (Cg. 2,000) per day or unusual pattern
High / Very High	All transactions subject to review

Other automatic flags include:

- No or limited gameplay before withdrawal
 - Use of multiple payment methods without clear purpose
 - Large bonuses followed by immediate cashout
-

4. Alerts and Case Management

Alerts are generated when pre-set rules or anomaly detection algorithms are triggered. The following steps are followed:

1. **Alert Generation:** Transaction is flagged by system
2. **Case Creation:** Alert is logged and assigned for review
3. **Preliminary Review:** AML Analyst checks transaction details, customer profile, and risk

score

4. **Information Gathering:** Request for SoF/SoW documents if needed

5. **Escalation:** If unresolved, case is escalated to the Compliance Officer for further analysis

Each alert must be resolved within 48 hours unless additional information is pending.

5. Review and Escalation Protocol

Upon review of flagged transactions, the decision tree is as follows:

- **No Risk Detected:** Case is closed with a documented justification
- **Low Risk / Justified Behavior:** Monitor account, file IUAR internally if needed
- **Medium to High Risk:** Escalate for EDD, freeze transaction temporarily
- **Suspicious Activity Detected:** Prepare and submit Suspicious Transaction Report (STR) or Unusual Transaction Report (UTR) to the FIU Curaçao

All escalations and outcomes are documented in the Company's case management system.

6. FIU Reporting Guidelines

Where transactions meet the criteria for unusual activity as outlined under NORUT:

- The Compliance Officer must submit a **UTR** to the **FIU Curaçao** within **48 hours**
 - All supporting documentation (KYC, transaction history, communications) must be attached
 - Internal records of IUARs and STRs are kept confidential and securely stored
 - Unauthorized disclosure ("tipping off") is strictly prohibited and subject to disciplinary action
-

7. Recordkeeping and Audit Trail

All transaction monitoring cases must be retained for **at least seven (7) years**. The following must be recorded:

- Alerts and related system logs
- Manual notes and reviews by staff
- IUARs and STR/UTR submissions
- Customer communications and responses
- FIU communications and follow-up actions

Audit trails are maintained in a centralized, secure system accessible only to the Compliance team.

8. Review and Enhancement

Transaction monitoring procedures and rule sets are reviewed **semi-annually** or upon:

- Regulatory updates
- Identified system weaknesses
- Audit or FIU feedback
- Emerging ML/TF typologies

Improvements may include new detection rules, updated thresholds, or integration of new third-party tools.

Know Your Customer (KYC) Policy

High Gaming IT Services BV

Effective Date: July 01, 2024

1. Objective & Scope

This Know Your Customer (KYC) Policy forms a core component of High Gaming IT Services BV's Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Program. The objective is to ensure that the Company identifies and verifies the identity of its customers, evaluates risk, and prevents the misuse of its services for illicit purposes including money laundering, terrorist financing, and fraud.

This policy applies to all customers and users of the Company's gaming platforms and financial transaction channels, including fiat and cryptocurrency services.

2. Identification Requirements

High Gaming IT Services BV requires all customers to provide the following information prior to engaging in financial transactions above the applicable thresholds:

- Full legal name
- Date of birth
- Nationality
- Residential address (no P.O. boxes)
- Email address and phone number
- Government-issued identification number

Customers are not permitted to maintain anonymous or fictitious accounts. Initial identification is required before account activation and/or first transaction. Additional documentation may be requested for high-risk customers or upon suspicion of unusual activity.

3. Verification Methods

Verification of customer identity shall be conducted using a combination of:

- **Documentary verification:**
 - Passport, national ID, or driver's license (must be unexpired and government-issued)
 - Utility bill or bank statement for proof of address (dated within last 3 months)
- **Non-documentary verification:**
 - Electronic identity verification via third-party services (e.g., Sardine A.I.)
 - Biometric verification (selfie with ID)
 - Database checks for PEPs, sanctions, and fraud alerts (e.g., Chainalysis, Dow Jones)

High-risk customers will be subject to enhanced procedures, including live ID checks, video verification, and collection of Source of Wealth (SoW) documentation.

4. Risk-Based Approach to KYC

High Gaming IT Services BV adopts a **risk-based approach** (RBA) to KYC compliance. Each customer is assessed and assigned a risk rating (Low, Medium, High, or Very High) based on the following factors:

- Geographic location and jurisdictional risk
- Source of funds or wealth
- Use of virtual assets or prepaid cards
- Behavioral patterns and transaction volume
- Association with PEPs or high-risk industries

The level of due diligence performed is commensurate with the assessed level of risk. High-risk customers are subjected to Enhanced Due Diligence (EDD), including SoW/SoF validation and management approval.

5. Recordkeeping Requirements

All records related to KYC activities, including customer identification, verification, and risk assessment, shall be retained for a **minimum of seven (7) years** from the date the account is closed or the transaction completed, whichever is later.

Documents retained include:

- Customer identification information and copies of documents
- Risk classification and KYC tier level
- Correspondence and compliance notes
- Logs of internal unusual activity reports (IUARs)
- Results of periodic reviews or re-verification

All records will be securely stored in digital format with restricted access.

6. Roles & Responsibilities

- **Compliance Officer (CO):**
Oversees the implementation and maintenance of the KYC Program. Reviews high-risk customer files, manages third-party verification services, and escalates issues to executive management as needed.
 - **Customer Onboarding Team:**
Responsible for collecting customer information and verifying documentation according to this policy.
 - **AML Analysts:**
Perform risk assessments, monitor customer activity, and flag any anomalies or red flags for further review.
 - **Executive Management:**
Approves the onboarding of PEPs and Very High-Risk customers.
-

7. Review & Updating of Customer Information

Customer records must be reviewed and updated:

- At least every 12 months for high-risk customers
- At least every 3 years for medium-risk customers
- Immediately upon a material change in behavior, funding method, or geographic risk
- When an alert is triggered by a third-party screening tool
- Upon failed verification or suspected fraud

The Company may suspend or terminate an account where a customer fails to comply with verification requests or provides misleading information.

8. Compliance and Enforcement

Failure to adhere to this policy may result in regulatory penalties, reputational damage, and account closure. Customers who refuse or are unable to provide adequate information will not be permitted to transact or continue using the platform.

All employees must receive annual KYC training and report any suspected violations to the Compliance Officer immediately.

Sanctions Compliance Policy

High Gaming IT Services BV

Effective Date: July 01, 2024

1. Overview of Sanctions Obligations

High Gaming IT Services BV is committed to ensuring full compliance with international sanctions regulations. This includes adhering to obligations set forth by the United Nations (UN), European Union (EU), United States Department of the Treasury's Office of Foreign Assets Control (OFAC), and other applicable jurisdictions. The purpose of this policy is to outline the procedures and responsibilities for identifying, screening, and managing sanctioned individuals, entities, and jurisdictions in connection with the Company's services.

2. Sanctions Lists Used

The Company screens individuals and transactions against the following key sanctions lists:

- OFAC Specially Designated Nationals (SDN) List
- EU Consolidated List of Sanctions
- United Nations Security Council Sanctions Lists
- Any additional national or regional sanctions lists applicable to the Company's operations

These lists are regularly updated and incorporated into the Company's screening tools through approved third-party providers (e.g., Chainalysis, Dow Jones, or equivalent).

3. Customer and Transaction Screening

Sanctions screening occurs at multiple stages of the customer lifecycle, including:

- At onboarding (during KYC)
- During transaction monitoring
- At withdrawal or payout events
- Periodically as sanctions lists are updated

The screening covers customer names, aliases, IP addresses, device IDs, wallet addresses, and transaction counterparties. Matches are automatically flagged and reviewed by the Compliance Officer or designated AML staff.

4. Handling Positive Matches

When a potential match is identified during sanctions screening:

- The account or transaction is immediately placed on hold
- The alert is escalated to the Compliance Officer for verification
- The customer is contacted only if necessary and in a manner that does not constitute "tipping off"
- No funds are disbursed or accounts unfrozen until the investigation is concluded

If the match is confirmed, the Company follows the appropriate reporting and freezing protocols.

5. Account Freezing Procedures

In the event of a confirmed sanctions match:

- The account and any associated funds will be immediately frozen in compliance with applicable laws
- The Company will notify relevant regulatory authorities (e.g., FIU Curaçao, OFAC)
- All attempts to access, withdraw, or move funds will be blocked
- Internal documentation will be maintained detailing the steps taken and notifications made

The account remains frozen until further instructions are received from the competent authorities.

6. Escalation and Reporting Protocols

Any positive or suspected match against a sanctions list is to be escalated immediately to the Compliance Officer. The Compliance Officer will:

- Document all findings and determine the legitimacy of the match
- Submit a report to the relevant authority if a match is confirmed
- Maintain strict confidentiality and ensure no unauthorized disclosures

All reports and internal decisions will be archived in accordance with the Company's Record Retention Policy.

7. Training & Awareness

All relevant employees are required to undergo sanctions compliance training as part of their AML/CTF training curriculum. The training includes:

- Overview of sanctions regimes and their implications
- Use of internal and third-party screening tools
- Identification of red flags and escalation procedures
- Prohibition on "tipping off" and guidance on confidentiality

Training is conducted at onboarding and on an annual basis thereafter. Additional targeted training may be conducted in response to regulatory updates or audit findings.

Internal Unusual Activity Report (IUAR) Form

High Gaming IT Services BV

Effective Date: July 01, 2024

Purpose

This form is used by employees of High Gaming IT Services BV to internally report suspicious or unusual activity that may indicate money laundering, terrorist financing, fraud, or other illicit financial activity. All submitted reports will be reviewed by the Compliance Officer. Reports must be submitted within 24 hours of identifying the unusual activity. All submissions will be kept confidential.

Internal Report Form

1. Date & Time of Report: _____
2. Reporting Employee Name: _____
3. Department / Position: _____
4. Customer Name: _____
5. Customer Account ID / Username: _____
6. Description of Unusual Activity:

7. Type of Suspicion (check all that apply):
 - ☐ Large or Unusual Withdrawal
 - ☐ Rapid Deposit Cycles
 - ☐ Use of Anonymous Funding Methods
 - ☐ Transaction Structuring
 - ☐ Unusual Gameplay Patterns
 - ☐ Other: _____
8. Date(s) of Suspected Activity: _____
9. Amount(s) Involved (if known): _____
10. Attached Supporting Documentation: ☐ Yes ☐ No
11. Additional Comments or Observations:

12. Employee Signature: _____ Date: _____

13. Confidentiality Notice: This report will be treated with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure is prohibited and may result in disciplinary or legal action.

AML/CFT Risk Assessment Template

High Gaming IT Services BV

Effective Date: July 01, 2024

Purpose

This AML/CFT Risk Assessment Template is designed to provide a structured framework for evaluating money laundering and terrorist financing risks at both the business and customer level. It helps to identify, assess, and document potential vulnerabilities and informs the development of appropriate mitigating controls.

1. Product/Service Risk

Evaluate the risk level associated with each of the products and services offered by the company, including online gaming, sports betting, cryptocurrency transactions, and fiat deposits/withdrawals.

- Are any products/services high velocity or cash-intensive?
- Do any allow anonymous or rapid transactions?
- Are there known fraud or abuse risks?

Risk Level: [Low / Medium / High]

Rationale:

2. Geographic Risk

Assess exposure to countries or regions considered high-risk due to inadequate AML/CFT laws, sanctions, or political instability.

- Does the Company accept customers from high-risk or sanctioned jurisdictions?
- Are there enhanced controls for non-EU, FATF-listed, or offshore regions?

Risk Level: [Low / Medium / High]

Rationale:

3. Customer Risk

Classify customer segments based on risk factors such as source of funds, occupation, nationality, and association with PEPs.

- What percentage of customers are high-net-worth, PEPs, or crypto-based?
- Is sufficient due diligence and monitoring applied?

Risk Level: [Low / Medium / High]

Rationale:

4. Delivery Channel Risk

Analyze how the Company's services are accessed and the risks associated with indirect, non-face-to-face, or third-party interactions.

- Are accounts opened and verified online only?
- Are third-party vendors used for onboarding, wallet services, or payments?

Risk Level: [Low / Medium / High]

Rationale:

5. Mitigating Controls in Place

Document existing internal controls that help mitigate the above risks.

- KYC and CDD Procedures
- Transaction Monitoring Systems
- Sanctions Screening
- Internal Reporting Mechanisms
- Employee Training and Testing

Effectiveness of Controls: [Weak / Adequate / Strong]

Supporting Evidence or Audit Results:

6. Overall Risk Rating & Rationale

Provide an overall risk rating for the Company's AML exposure and justification.

Overall Risk Rating: [Low / Medium / High / Very High]

Summary of Rationale:

Date of Assessment: _____

Assessed By: _____

Approved By: _____

AML Employee Training Manual

High Gaming IT Services BV

Effective Date: July 01, 2024

1. AML/CTF Overview

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) refer to the laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income and to prevent the financing of terrorist activities. High Gaming IT Services BV is committed to maintaining a robust AML/CTF compliance framework aligned with international standards and national laws.

2. Red Flags and Suspicious Behavior

Employees should be vigilant for signs of suspicious activity, including:

- Unusually large or structured transactions
- Reluctance to provide identification or documentation
- Use of multiple accounts without clear reason
- High-value withdrawals after limited gameplay
- Use of anonymous funding sources or crypto wallets
- Transactions to or from high-risk jurisdictions

If in doubt, escalate the matter to the Compliance Officer.

3. Steps for Reporting Suspicious Activity

All employees are required to report suspicious activity using the **Internal Unusual Activity Report (IUAR) Form**. The reporting process is as follows:

1. Observe and document the activity
2. Complete the IUAR form with as much detail as possible
3. Submit the form to the Compliance Officer within 24 hours
4. Do not disclose to the customer or third parties that a report has been made (no tipping off)

The Compliance Officer will investigate and determine whether a report to the FIU is necessary.

4. Role of the Compliance Officer

The Compliance Officer is responsible for:

- Overseeing the AML/CTF compliance program
 - Reviewing internal reports of suspicious activity
 - Filing necessary reports to the Financial Intelligence Unit (FIU)
 - Coordinating employee training and periodic testing
 - Ensuring compliance with sanctions and legal obligations
-

5. Sanctions Awareness

Employees must understand that it is prohibited to conduct business with individuals or entities subject to international sanctions. These include but are not limited to the OFAC, UN, and EU sanctions lists.

Employees must screen customers, counterparties, and transactions to ensure no sanctioned persons are served. Any positive match must be immediately reported to the Compliance Officer.

6. Annual Training Requirements

All employees must complete AML/CTF training upon onboarding and annually thereafter. Training content includes:

- Overview of AML/CTF laws and internal procedures
- Case studies and red flag recognition
- Sanctions compliance requirements
- Use of internal reporting tools

Attendance is mandatory and documented. Failure to complete training may lead to disciplinary action.

7. Quiz/Assessment Section

Please complete the following questions to assess your understanding of AML/CTF procedures:

1. What is considered a red flag for suspicious activity?
2. When should you submit an IUAR form?
3. What is "tipping off" and why is it prohibited?
4. Who should you contact if a customer appears on a sanctions list?
5. What are the consequences of non-compliance with AML rules?

Employee Signature: _____

Date: _____

Customer Risk Assessment (CRA) Procedures

High Gaming IT Services BV

Effective Date: July 01, 2024

1. Purpose

The Customer Risk Assessment (CRA) Procedure outlines how High Gaming IT Services BV assigns, monitors, and updates risk levels associated with individual customers. This is essential to ensure that appropriate due diligence, monitoring, and controls are applied according to the customer's risk profile, in compliance with AML/CTF laws and the Company's internal policies.

2. Risk Indicators

Each customer is evaluated based on a range of risk indicators grouped into three primary categories:

2.1 Behavioral Indicators

- Rapid deposit or withdrawal activity
- Minimal gameplay with significant financial transactions
- Repeated attempts to avoid verification
- Use of multiple accounts or identities

2.2 Geographic Indicators

- Customer resides in, is a citizen of, or transacts with high-risk jurisdictions
- Use of VPNs to mask real location
- Associations with countries listed by FATF, OFAC, or other sanctions regimes

2.3 Funding Source Indicators

- Use of anonymous or unregulated payment methods (e.g., crypto mixers, pre-paid cards)
 - Undocumented or unverifiable source of funds
 - Significant deposits inconsistent with income or declared occupation
-

3. CRA Scoring Mechanism

The CRA assigns a **numerical or categorical risk score** to each customer using a weighted system that combines the indicators above.

Risk Tiers:

- **Low Risk** – Fully verified customers using regulated payment methods from low-risk jurisdictions
- **Medium Risk** – Customers with minor risk indicators or incomplete profiles pending resolution
- **High Risk** – PEPs, customers from sanctioned jurisdictions, or those with behavioral red flags
- **Very High Risk** – Confirmed sanctions matches, fraud suspects, or customers flagged by law enforcement

Scores are automatically influenced by real-time data feeds from verification vendors (e.g., Sardine A.I., Chainalysis) and are reviewed manually by the Compliance team as needed.

4. Initial Risk Rating at Onboarding

Upon account creation, all users are given a preliminary risk score based on:

- Verification completeness (ID, address, age)
- Funding method
- Country of registration/IP address
- PEP/Sanctions screening outcome

No user is permitted to transact until a risk score is generated and minimum KYC thresholds are met.

5. Triggers for CRA Re-evaluation

A customer's risk level must be re-assessed when any of the following occur:

- Cumulative deposits exceed USD 2,000 (or Cg. 4,000 equivalent)
 - An attempted withdrawal is initiated
 - A suspicious pattern or transaction is detected
 - The customer updates their personal or payment information
 - Alerts are received from vendors or internal monitoring tools
 - The customer is flagged for Enhanced Due Diligence (EDD)
-

6. Documentation and Escalation Process

Each risk assessment and its changes must be documented, including:

- Risk classification assigned
- Indicators used and rationale
- Reviewer(s) and timestamps
- Any supporting documents received

Escalation:

- Medium and High-risk accounts are reviewed by the Compliance Officer
- Very High-risk or PEP accounts require executive approval prior to full activation
- Internal Unusual Activity Reports (IUARs) must be filed where suspicion exists

All records are retained for at least **seven years** from the last interaction or account closure.

7. Enhanced Due Diligence (EDD) Procedures

For high or very high-risk customers, the following EDD measures apply:

- Verification of source of wealth and income
- Live video or biometric verification
- Explanation of purpose and anticipated use of account
- Transaction pattern justification
- Ongoing review frequency increased (e.g., every 3 months)

EDD must be completed and approved before any significant transactions (withdrawals or large deposits) are allowed.

8. Review and Audit

The CRA process is reviewed **annually** and during any regulatory audit. Random spot checks are performed monthly to ensure procedural compliance and accuracy of risk classifications.