**Betelgeuse Entertainment B.V.**

**Anti-Money Laundering and Prevention of Crime Policy**

1. **Objectives**

The aim of this document is to define the policy and procedures in relation to risk assessment and management and involves a number of discrete steps in assessing how to manage and mitigate the money laundering and terrorist financing risks faced by Betelgeuse Entertainment B.V. (**the “Company**”). The Company is committed to prevent gambling from being a source of crime or disorder, being associated with crime or disorder, or being used to support crime.

1. **The meaning of money laundering**

The Company operates under the National Ordinance on Identification when rendering the services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92), the National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99), National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282) and the National Decree supervisor unusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector, LB van 28 januari 2019, no. 19/0283).

Money laundering covers wide-ranging circumstances involving any activity concerning the proceeds of crime and includes:

* trying to turn money raised through criminal activity into ‘clean’ money,
* possessing or transferring the benefit of acquisitive crimes such as theft and fraud, and funds generated from crimes like tax evasion (this includes the possession by an offender of the proceeds of his own criminal activity),
* possessing or transferring stolen goods,
* being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property,
* criminals investing the proceeds of their crimes in the whole range of financial products.
* entering into arrangements to facilitate the laundering of criminal or terrorist property.

There are two main forms of money laundering in the gambling sector:

* exchanging money, assets, goods and property that were acquired criminally for money or assets that appear to be legitimate or clean, achieved by transferring or passing the funds through some form of legitimate business transaction or structure,
* the use of criminal proceeds to fund gambling as a leisure activity.

Money laundering is considered to be an offence by law. Money laundering covers wide ranging circumstances involving any activity concerning the proceeds of crime and includes:

* attempting to turn money acquired through criminal activity into ‘clean’ money,
* possessing or transferring the benefit of acquisitive crimes, such as theft and fraud,
* possessing/transferring stolen goods,
* being directly involved with any criminal or terrorist property,
* entering into arrangements to facilitate the laundering of criminal or terrorist property.
1. **AML offences**

Offences in relation to money laundering include:

* concealing criminal property,
* disguising criminal property,
* converting criminal property,
* transferring criminal property,
* removing criminal property;
* offences of failing to report suspected money laundering,
* offences of tipping off about a money laundering disclosure, tipping off about a money laundering investigation and prejudicing money laundering investigations,
* acquiring, using or possessing criminal property,
* entering into or becoming concerned in an arrangement which the person knows or suspects facilitates the acquisition, retention, use or control of criminal property,
* tipping off a person that a report has been made.

Traditional money laundering and terrorist financing methods:

* winnings or unused funds withdrawn to an account other than the one from which the original deposit was made;
* manipulation of financial intermediaries;
* account hijacking or hacking (account takeover);
* legal and illegal betting (match fixing);
* holding accounts (holding illegitimate funds in accounts without intention to bet or stake);
* peer to peer games collusion (the agreement between two or more parties to bet and play in pre - determined pattern unbeknown to the operator and / or other participants.
1. **Organisation and Personal Risk**

Money laundering and terrorist financing carry a wide array of risk where on organisation or employee is seen to be complaint or negligent, the risk are interdependent:

*Financial Risk:*

* fines from criminal convictions;
* fines from the regulator;
* loss of position within the organisation due to misconduct;
* loss of business due to proceeding against the organisation.

*Regulatory Risk*

* the organisations’  regulatory status being regarded as at risk;
* loss of licence;
* sanctions against the organisation.
1. **Responsibilities**

The relevant department is responsible for monitoring all transactions to and from the Company and verifying the identity of all online registered players that reached set threshold. The Company’s senior management, as well as all employees, are fully committed to adopting a risk-based approach to anti-money laundering (“**AML**”) with effort focused where it is most needed to be able to process payment transactions between the Company and customers in a way free of money laundering matter issues.

The developed internal systems and procedures applied by the Company are appropriate for remote gaming businesses. The Company appreciates that its money laundering and terrorist financing risk assessment is not a one-off exercise, and these are assessed regularly so that adopted approach is effective at any time.

**5.1. Senior Management Responsibility**

Senior management is fully engaged in the processes around the Company’ assessment of risks for money laundering and terrorist financing and are involved at every level of the decision making to develop the appropriate policies and processes to comply with relevant legislation.

**5.2 Money Laundering Reporting Officer (“MLRO”)**

The MLRO is responsible for the oversight of all aspects of the AML activities within the company and has the authority to act independently in carrying out his responsibilities having access to sufficient resources to carry out his duties. His duties and responsibilities include:

* identifying money laundering and terrorist financing risks relevant to the Company;
* designing and implementing policies and procedures relating to AML and countering terrorist financing (“**CTF**”), monitoring the effectiveness of these and reviewing and updating these policies and procedures;
* reporting to Senior Management on AML and CTF activity and the effectiveness of the Company’s controls;
* keeping AML/CTF records;
* receiving internal disclosures and deciding whether these should be reported;
* training employees to ensure that they are aware of the Company’s AML policies and
* procedures and how to report suspicious transactions;
* being the internal point of contact for the suspicious transaction reports (“**STRs**”);
* reviewing and investigating STRs and considering whether a suspicious activity report (“**SAR**”) should be submitted to the authorities.

Any internal report should be considered by the nominated officer, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

Where any AML tasks are delegated within the business, the MLRO will remain responsible for all AML issues. Any delegated tasks will be recorded and will be countersigned by the delegate to confirm acceptance of responsibility. Employees who need to be aware of the delegation will be notified immediately.

**5.3 Employees’ Responsibilities**

Employees are trained to follow the Company’ policies and procedures for customer due diligence and ongoing monitoring processes.

Employees must report to the MLRO any knowledge or suspicion of money laundering whether by customers, guests or other employees by drafting an internal STR.

1. **Customer Due Diligence (“CCD”)**

Identifying a customer means obtaining information about his identity (name, address, date of birth, employment and financial history, physical appearance and family circumstances).

Verifying identity means obtaining evidence that supports this information.

* one government document which verifies either name and address or name and date of birth; or
* a government document which verifies the customer’s full name and another supporting document which verifies their name and either their address of date of birth.

CDD is carried out to identify and verify the identity of all customers who:

* withdraw the funds in any amount;
* approach the deposit threshold of 2,000 EUR.

The Company is aware that CDD is ongoing and may need updating where there are changes in a customer’s circumstances and personal details.

The CDD includes the customer’s name, plus residential address, photo and date of birth proved by an identification documents, and, in some circumstances when requested by the Payment Department, a copy of the payment method used or to be used by the customer.

When CDD checks on an existing customer have been completed within one of the Company’s products, CDD will not be conducted again in relation to another product unless a different payment method is used by the customer.

* 1. **Customer Registration**

In order to open an account with the Company at the web portal playbison.com, a customer must first complete the registration process.

The registration details to be filled in by all new customers include the username, password, first and last name, address, country of residence, date of birth, e-mail address or mobile phone number, and account currency. During registration, customer identification takes place by way of the age verification process.

When a new account is created, a verification activation code is sent to the phone number or e-mail  specified during the registration process. When the user enters the activation code, the account is then successfully created. Only at this point can the customer deposit money and start placing bets.

Customers must be at least 18 years old and are permitted to register only one player account in their name. No underage users are allowed to play on the websites. The Company is committed to prevent underage persons from using its gambling facilities, and will take all necessary steps to ensure they do not register with its remote gaming website. Users who do not have a registered player account will not be allowed to play casino games or place bets.

List of countries from which players are not allowed to be registered is available in Annex 1, attached to this procedure.

* 1. **Documentary evidence**

The Company relies upon documents issued by government departments during CDD.

To fulfil the necessary customer identification and verification process, the Company requires its customers to upload on their websites (under My account -> My documents) a copy of valid identification documents. This request is communicated to the customer via the email address registered. If necessary, the customer may be contacted by phone to further facilitate and enable the verification process. If documents are in a foreign language, the Company takes appropriate steps to be reasonably satisfied that the documents provide evidence of the customer’s identity, for example, by obtaining a translation of the relevant sections. Such a step would be to request that the customer provide the documents with a certified true translation.

Only documents issued by government departments and agencies that contain a photograph are considered reliable to verify the customer’s identity. Government issued documents without a photograph may be used to confirm the current address of the customer (if stated on the document).

The following sources may be accepted for verification of customers:

* current passport;
* current photo card driving licence;
* residence permit;
* ID card;
* council tax bill;
* utility bill;
* bank, credit card, building society or credit union statement;
* local council or housing association rent card or tenancy agreement;
* house or motor insurance certificate.
	1. **Enhanced due diligence (“EDD”)**

Under the Regulations, there are following circumstances in which EDD on customers should be carried out, which goes beyond identifying them and verifying their identity. These are:

* when the customer is a PEP;
* in any other situation where the customer presents a higher risk of money laundering or terrorist financing (e.g. a high spending customer).

In relation to PEPs and other customers that present a higher risk of money laundering or terrorist financing, the Company will seek to obtain evidence of the customer’s source of funds. This evidence may include:

* Identification documents provided by the customer (e.g. passport, driving licence, utility bill);
* Business cards provided by the customer;
* Information provided by the customer in conversation;
* Verification of identity using an online provider;
* Third party acuity and wealth reports;
* Credit reports;
* Information available in the media and on the internet;
* Search of PEP databases;
* Company registration searches for companies the customer appears to be a shareholder or officer.

The Company will use a mix of sources, including external sources and information taken directly from the customer, for EDD purposes.

* 1. **Requirements procedures**

In the light of the requirements imposed by law and regulations, the Company adopts the following procedure when CDD is triggered:

* at the point that verification is triggered, the Company shall not proceed with any withdrawal until the account is fully verified;
* further deposits can be made to that account as long as they too are ‘locked’ into it until CDD is completed;
* bets can be made from the account, again providing any winnings are ‘locked’ until CDD is completed;
* once CDD is completed, the account can be ‘unlocked’ and business can continue as normal;
* if CDD cannot be completed, then the Company will terminate the business relationship with the customer;

Risk assessments are undertaken which include the following:

* multiple destinations – is the customer requesting that the money be sent to several bank accounts;
* high risk destination – is the customer requesting that the money be returned to a country where there is a significant money laundering concern;
* unusual patterns and large transactions - is there an apparent economic or lawful purpose behind the transactions;
* very high account turnover - is the turnover consistent with the balance;
* irregular activity - are the transactions outside of the customer’s regular transaction activity;
* ongoing monitoring of the customer’s account and activity.

Customer risk assessment is based on the below factors:

*Customer risk*

In order to categorize the players whose activities may indicate a higher risk we scrutinize players who are:

* PEPs, family members of PEPs or known close associates of PEPs;
* high or disproportionate spenders;
* display changing or unusual spending patterns;
* have international sanctions;
* using third party payment methods;
* register multiple player accounts to hide their spending levels or to avoid breaching the CDD threshold;
* not easily found in open source checks/ whose occupation is unknown.

*Transaction risk*

Higher risk posed by multiple gambling accounts or wallets; players using a number of bank accounts and payment methods; use of prepaid cards and e-wallets; high or unusual payments;  total number of deposit and withdrawal methods; discrepancies between available income information (open source/ declaration) and depositing sums.

The higher the complexity and number of payment methods, the higher the risk should be.

*Product risk*

The Company offers casino and live casino only which is deemed as a low risk.

Employees remain vigilant and use their experience and common sense in applying the Company risk-based criteria and rules, using guidance from the senior management MLRO or other nominated officer as appropriate.

* 1. **Failure to complete checks**

If customer of the Company is unable to comply with or complete the required CDD or EDD, the Company will not carry out a transaction with or for the customer through any of the available payment methods. Instead, the customer’s account will be terminated and the Company will consider making a report to the relevant authority if there is any sign of money laundering activity.

All the Company relevant staff understand that it is an offence to tip off a person that a report has been made. Staff are trained to understand that they must not inform or warn a customer that their transactions have been noted and/or reported, either internally or externally.

1. **Ongoing Monitoring**

Monitoring customer activity is carried out using the risk-based approach, with higher risk customers, such as PEPs, being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than is appropriate for lower risk customers. Monitoring of customers is done by the relevant employees who monitor customer activity live.

**7.1. Supporting records**

The website playbison.com will, by the nature of their business, generate detailed records of all transactions with each customer and for purposes of the record keeping requirements the Company retains the drop/win figures for each named customer.

1. **Training**

All relevant employees of the Company are given training on AML and CTF, both at induction and by way of refresher training on an annual basis. The Company ensures that employees understand the Regulations and apply the Company’s policies and procedures, including the requirements for CDD and, record keeping and STRs/SARs.

The MLRO, nominated officers and employees responsible for completing CDD checks are regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

1. **Record Keeping**

The Company will keep records of the following:

* Customer interactions - Details of all customer interactions and relationships including which employee dealt with the interaction, what was asked, why an interaction was made and the outcome of the interaction.
* MLRO - The decision made when receiving a STR, training received from external organisations and given to employees, details of AML tasks assigned to employees, reports sent to the authorities, decisions made by the authorities on SARs and the action the Company will take after the authorities has made their decision.
* Risk-based approach - Details of steps taken to manage and mitigate risks of crime and disorder.
* Customer identification and verification information, including copies of any enhanced due diligence documentation.

These records will be kept for a period of at least 5 years.

1. **Reporting**

Where an employee of the Company has received information, as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, that employee must make an internal note report and inform a senior management, an STR, to the MLRO.

Any STRs are considered by the MLRO, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing. Where appropriate, the MLRO will make a SAR to the relevant authority and will apply for the appropriate consent required.

1. **Collusion and cheating**

The Company has systems to detect cheating, collusion or illegal activity, including suspicious and large transaction alerts, risk management solutions to monitor customer transactions and online risk solutions. Where suspicious activity is identified, the customer’s account will be reviewed and this will be reported to the management as an STR to the MLRO. The customer’s account will be suspended and where cheating/collusion is identified, the account will be closed and the customer will be reported, where it is deemed necessary.

If an employee is implicated in any cheating, collusion or other illegal activity, they will be suspended pending a full investigation.

1. **Protection of equipment**

The Company ensures that its equipment and business is protected from crime and criminal misuses by:

* keeping its premises fully locked when no member of staff is present.
* members of staff access the office by using an in-out log. This will allow tracking of staff members in case of illegal activity.
* computer equipment is protected by user-log out and password protected screensavers whenever it is left unattended, or outside office hours.
* the office premises are kept secure.
1. **Domain list**

The company operates the following domains

1. Playbison.com
2. Playbull.vip
3. Bison.win (pending)

|  |
| --- |
| **DOCUMENT CREATION** |
| **Version**  | 2.0 |
| **Date Created** | 1 January 2023 |
| **Author(s) of Document** | Paweł Piętak, MLRO |
| **Purpose of Document** | This policy is aimed at defining the manner by which the business conducts operations procedures towards Anti-Money Laundering, Fraud and Counter Financing of Terrorism. Where specific business lines or country-level AML/CFT Laws require more, those requirements will apply in addition to the minimum standards identified here. |
| **Authorised By** | Paweł Piętak, MLRO |
| **CHANGE CONTROL** |
| **Version** | **Date of Issue** | **Author(s)** | **Brief Description of Changes** | **Approved By** |
| 1.0 | 1 December 2022 | Paweł Piętak | Initial Release | Paweł Piętak |
| 2.0 | 1 January 2023 | Paweł Piętak | Updated document as per procedures changes | Paweł Piętak |
| 2.1 | 31 May 2023 | Paweł Piętak | Restricted territories list update | Paweł Piętak |
| 2.2 | 11 January 2024 | Paweł Piętak | Restricted territories list update- list moved to a separate Annex 1 document. | Paweł Piętak |
| 2.3. | 15 January 2024 | Paweł Piętak | New domains | Paweł Piętak |