

# **Blue Pepper B.V.**

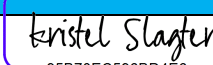
## **Anti-Money Laundering and Countering the Financing of Terrorism Manual *(Curacao)***

Version 5.0

**Document Information**

|                                |                                                                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject</b>                 | AML/CFT Manual – version 5.0                                                                                                          |
| <b>Purpose</b>                 | Guidance manual and policy stance detailing how the company complies with its legal and regulatory obligations in respect of AML/CFT. |
| <b>Document Owner</b>          | Compliance – for any questions regarding this policy please contact Compliance at email <b>compliance@bluepepperbv.com</b>            |
| <b>Review</b>                  | Annually or earlier upon significant business changes which have an impact on AML/CFT.                                                |
| <b>Involvements</b>            | All operational departments.                                                                                                          |
| <b>Approval</b>                | Director                                                                                                                              |
| <b>Document Classification</b> | Internal Use                                                                                                                          |

**Approval**

| <b>Date</b> | <b>Version</b> | <b>Title</b> | <b>Signature</b>                                                                                                                               |
|-------------|----------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 1/14/2026   | 5.0            | Director     | <div>Ondertekend door:</div>  <div>95B70EC596BD4E6...</div> |

**Version Control**

| <b>Version No</b> | <b>Date</b> | <b>Title</b> | <b>Description</b>                                                                                                                                                                                                                                    |
|-------------------|-------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0               | 30/08/24    | Compliance   | New policy incorporating latest regulatory requirements.                                                                                                                                                                                              |
| 2.0               | 26/02/25    | Compliance   | Review and update – Reference to the Cryptocurrency Policy; Additional information on the PEP and Sanction screening process; Details regarding a new e-learning platform which provides bespoke AML/CFT training in relation to Curacao legislation. |
| 3.0               | 23/04/25    | Compliance   | <p>Review of latest AML policy issued by the CGA to ensure this policy meets all the necessary elements.</p> <p>Updates include the inclusion of Compliance contact information and</p>                                                               |

|     |          |            |                                                                                                                                                                      |
|-----|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |          |            | the requirements to provide information and documentation to the GCB at point 8.4.                                                                                   |
| 4.0 | 02/10/25 | Compliance | Additional information relating to the transaction monitoring regime (4.5.1), EDD arrangements (4.6), Details of the customer risk scoring tool (5.3).               |
| 5.0 | 14/01/26 | Compliance | Adjustment to the documents accepted to verify POA (4.3.1), and minor additions throughout to ensure that the policy follows the CGA AML policy requirement feedback |

Table of Contents

**SECTION 1 – PURPOSE TO THE AML/CFT MANUAL & OBJECTIVES ..... 6**

1.1 Purpose of the AML/CFT Manual..... 6

1.2 Policy Statement and Objectives ..... 6

**SECTION 2 – BACKGROUND TO MONEY LAUNDERING AND TERRORIST FINANCING ..... 7**

2.1What is money laundering (I.2 – AML regulations) ..... 7

2.1.1 Placement ..... 7

2.1.2 Layering..... 7

2.1.3 Integration ..... 8

2.2 Terrorist Financing (I.3 – AML regulations) ..... 8

2.3 Sanctions (I.5 – AML regulations) ..... 8

2.4 Proliferation Financing (I.4 – AML regulations) ..... 8

**SECTION 3 – LEGISLATION AND FRAMEWORK..... 9**

3.1 Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, January 2025 (“AML regulations”) ..... 9

3.2 National Ordinance on identification when rendering services (N.G. 2017, no. 92) ..... 9

3.3 National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99) ..... 9

3.4 Sanctions National Ordinance (N.G. 2014, no.55) and the Kingdom Sanction Act (N.G. 2016, no.54) ..... 9

**SECTION 4 – CUSTOMER REGISTRATION, VERIFICATION, and POLICY ON CUSTOMER ACCEPTANCE (III.2.1 and III.2.2 – AML regulations) ..... 9**

4.1 Customer registration and identification ..... 9

4.1.1 Nature of customer (III.2.2 – AML regulations) ..... 10

4.1.2 Geolocation block / IP detection ..... 10

4.1.3 Device detection ..... 10

4.1.4 Automated duplicate account prevention ..... 11

4.1.5 Manual duplicate account detection (III.1 – AML regulations) ..... 11

4.2 PEP and Sanction screening ..... 11

4.3 Verification Documents ..... 12

4.3.1 Acceptable ID and POA ..... 12

4.4 Payments..... 12

4.4.1 Cryptocurrency ..... 13

4.4.2 Proof of Deposit ..... 14

4.5 Ongoing Monitoring (III.2.4 – AML regulations)..... 14

4.5.1 Transaction monitoring ..... 14

4.5.2 Risk based events..... 14

|                                                                                                    |           |
|----------------------------------------------------------------------------------------------------|-----------|
| 4.6 Enhanced due diligence (III.4 – AML regulations) .....                                         | 15        |
| 4.6.1 Triggers for enhanced due diligence .....                                                    | 15        |
| 4.6.2 Enhanced due diligence requirements .....                                                    | 15        |
| 4.6.3 Failure to meet EDD requirements and termination of the business relationship (III.8) .....  | 16        |
| <b>SECTION 5 – RISK ASSESSMENTS.....</b>                                                           | <b>16</b> |
| 5.1 Business Risk Assessment (II.2.1 – AML regulations) .....                                      | 16        |
| 5.2 Technical developments risk assessment (II.2.3 – AML regulations) .....                        | 16        |
| 5.3 Customer Risk Assessment (II.2.2 – AML regulations) .....                                      | 17        |
| 5.3.1 High Risk factors.....                                                                       | 17        |
| 5.3.2 Geographical risk factors (II.2.3.2 – AML regulations).....                                  | 18        |
| <b>SECTION 6 – RECORD KEEPING (IV.3 – AML regulations).....</b>                                    | <b>18</b> |
| 6.1 Identity Records .....                                                                         | 18        |
| 6.2 Transaction Records.....                                                                       | 19        |
| 6.3 Record retention .....                                                                         | 19        |
| <b>SECTION 7 – INTERNAL &amp; EXTERNAL REPORTING PROCEDURES.....</b>                               | <b>19</b> |
| 7.1 Compliance officer (V.3 – AML regulations) .....                                               | 19        |
| 7.2 Potential Suspicious Events (red flags) .....                                                  | 20        |
| 7.3 Internal Reports (IV.1 – AML regulations) .....                                                | 20        |
| 7.5 Register of money laundering, financing of terrorism and proliferation financing reports ..... | 22        |
| 7.5.1 External reports (IV.1 – AML regulations) .....                                              | 22        |
| <b>SECTION 8 – STAFF, TRAINING AND MONITORING COMPLIANCE (V.4 – AML regulations).....</b>          | <b>23</b> |
| 8.1 New staff appointments .....                                                                   | 23        |
| 8.2 Staff Training .....                                                                           | 23        |
| 8.2.1 Compliance Academy .....                                                                     | 23        |
| 8.2.2 Compliance Knowledge Hub .....                                                               | 24        |
| 8.2.3 Ad hoc and bespoke training .....                                                            | 24        |
| 8.3 Testing of the AML program (V.5 - AML regulations) .....                                       | 24        |
| 8.4 Examination by the Gaming Control Board (V.6 - AML regulations) .....                          | 25        |
| <b>SECTION 9 – APPENDICES .....</b>                                                                | <b>25</b> |
| 9.1 Appendix 1 – Politically Exposed Persons (III.6 – AML regulations) .....                       | 25        |
| 9.1.1 Politically Exposed Person .....                                                             | 25        |
| 9.1.2 PEP definition according to Annex 1 of the AML regulations.....                              | 26        |
| 9.2 Appendix 2 – SAR Internal Reporting Form .....                                                 | 26        |
| 9.3 – Appendix 3 – Curacao Financial Intelligence Unit Online Reporting System .....               | 26        |

## **SECTION 1 – PURPOSE TO THE AML/CFT MANUAL & OBJECTIVES**

### **1.1 Purpose of the AML/CFT Manual**

The purpose of this manual is to:

- Provide guidance and advice to staff and to demonstrate to relevant authorities the obligations Blue Pepper B.V. have as an online gambling license holder in Curaçao.
- Provide a high-level reference to the internal policies and procedures that are in place to ensure compliance with these requirements.

The contents of this manual reflect the requirements of all applicable legislation and regulation including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting Unusual Transactions (NORUT), the Sanction National Ordinance, and the Kingdom Sanction Act.

Reference is made within this manual to the internal measures, policies and procedures that are put in place to comply with license obligations.

### **1.2 Policy Statement and Objectives**

The Company is determined and committed to prevent the carrying out of financial activities through its systems that may be related to Money Laundering (ML)/ Financing of Terrorism (FT)/ Proliferation Financing (PF).

The Company recognizes its duty to comply with its obligations in law by having the necessary and relevant processes to prevent ML/FT/PF and to ensure that any suspicious activities are escalated to the authorities.

It is the policy of the Company that all staff shall positively participate in preventing the services of the firm from being exploited by criminals and terrorists for the purposes of money laundering and/or terrorist financing.

The objectives of this participation shall be:

- Ensuring compliance with applicable laws, statutory instruments, and requirements of the Curacao Gaming Authority;
- Protecting the Company and its staff from the risks associated with breaches of law and regulations;
- Mitigating the risk of reputational damage resulting from money laundering and terrorist financing by making a positive contribution to the fight against crime.

To achieve the above objective, it is Blue Pepper's policy that:

- Staff are aware of and demonstrate meeting their personal obligations as required by law or applicable to their role and position;
- Commercial decisions shall never take precedence over the company's commitment to the fight against money laundering and terrorist financing or financial crime;
- The company shall appoint a compliance officer who shall be afforded the assistance and cooperation of all staff in carrying out the duties of this appointment;
- Not knowingly establish an account or relationship with a customer that is a suspected or known criminal, holds PEP status, or is subject to EU, UN, or Curacao financial sanctions.

The Board of Directors has overall accountability for AML/CFT governance and the approval of the AML/CFT program. Day-to-day implementation is delegated to the Compliance Officer, who reports regularly to the Board on the effectiveness of controls, material risks, breaches, and regulatory developments.

## **SECTION 2 – BACKGROUND TO MONEY LAUNDERING AND TERRORIST FINANCING**

### **2.1 What is money laundering (1.2 – AML regulations)**

Money Laundering is generally defined as engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally delivered proceeds so that those proceeds appear to have been derived from legitimate activities or otherwise constitute legitimate assets.

The launderers objectives are to disguise and conceal the origin of the criminal proceeds, to avoid detection, and to benefit from the proceeds. On occasion this financial benefit may simply be utilizing criminal funds in gameplay.

#### **2.1.1 Placement**

The stage whereby the proceeds of crime enter the financial system. Traditionally, 'placement' may involve a wide variety of techniques, from large cash deposits to smaller deposits made through third party banks, and payment service providers.

#### **2.1.2 Layering**

The criminal property is separated from the initial entry to the financial system. This involves the creation of additional layers to try and disguise the audit trail to provide legitimacy to the

proceeds and confuse any audit trail.

### **2.1.3 Integration**

The laundered proceeds are returned to the legitimate economy having been layered and cleaned to make them appear they are from a legitimate source.

It is important to note that money laundering does not always occur in such a neat 3 stage process and involves all types of property and not just cash.

## **2.2 Terrorist Financing (I.3 – AML regulations)**

The funding of terrorism is the process of making funds or other assets available to support, even indirectly, terrorist activities. Many of the controls implemented serve the dual purpose of combating both ML/FT. Whereas ML is the process of making dirty money appear legitimate, FT attempts to use money which may be either legitimate or illegitimate for the purposes or activities of terrorist groups.

## **2.3 Sanctions (I.5 – AML regulations)**

Sanctions are punitive measures taken against a country, individual, legal persons, or organisations with the aim of maintaining or restoring international peace and security. Sanctions can be placed on sectors, industries or interests and generally target specific individuals or entities of those sectors.

**The Company is bound by all EU, UN, and Curacao sanctions regimes. Individuals who are detected as being named on any such financial sanctions lists shall not be accepted as customers. In the event a customer is accepted and subsequently appears on such a list then the account must be immediately blocked, funds restricted, and an Internal Suspicion Report submitted to the compliance officer.**

## **2.4 Proliferation Financing (I.4 – AML regulations)**

Proliferation is defined by FATF as the illegal 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.

Proliferation is often linked to the mass production of Weapons of Mass Destruction (WMD) and their means of delivery and related materials, in contravention of domestic law and/or interactional obligations. WMD's are designed to kill, bring serious harm to numerous individuals, and cause severe damage to artificial structures, natural structures, or the biosphere.

It is important that all staff are mindful of the risk of our customers being involved in such activities so that any concerns can be escalated to the compliance officer without delay. Red flags may include: -

- Customers involved in activities involving the use of dual use goods (*items which can be used for both civilian and military use*);
- Customers involved with shell companies and the use of Po Box addresses;
- Open-source intelligence indicates the customer is linked to shipping activities in high risk or sanctioned countries;
- Customers subject to relevant adverse media or a Sanctions match are detected via our screening provider.

FATF Guidance on Counter Proliferation Financing is available by accessing this [link](#).

## **SECTION 3 – LEGISLATION AND FRAMEWORK**

This section provides a list of the core AML/CFT legislation currently in place in Curacao, and reference should be made to the legislation for a fuller understanding of the requirements.

It is important that all staff familiarise themselves with the legislation and understand their personal obligations and responsibilities.

### **3.1 Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, January 2025 (“AML regulations”)**

### **3.2 National Ordinance on identification when rendering services (N.G. 2017, no. 92)**

### **3.3 National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)**

### **3.4 Sanctions National Ordinance (N.G. 2014, no.55) and the Kingdom Sanction Act (N.G. 2016, no.54)**

## **SECTION 4 – CUSTOMER REGISTRATION, VERIFICATION, and POLICY ON CUSTOMER ACCEPTANCE (III.2.1 and III.2.2 – AML regulations)**

### **4.1 Customer registration and identification**

Players are required to complete the registration process to perform any financial activity or gameplay. During the registration process, the following information is required to complete the registration:

- First name;
- Last name;
- Date of Birth;
- Email address;

- Password;
- Residential address;
- Post code;
- Country;
- Mobile phone number;
- IP address (captured);
- Device information (captured);
- Acceptance of the Terms and Conditions.

The company's systems do not allow persons under 18 years of age to register.

In accordance with the company's terms and conditions, if on completion of our verification checks, the account or the payment methods used by the user are suspected to belong to an individual under 18 years of age:

In accordance with departmental procedures, the under-age customer shall be offboarded, and their account is closed.

#### **4.1.1 Nature of customer (III.2.2 – AML regulations)**

The Company does now allow registrations and will not conduct any transactions from business customers, corporate entities, legal arrangements, trusts, foundations or similar.

The Company exclusively offers its services to customers with an established customer relationship (i.e., the customer must be registered and hold an account with the Company) and offers its services for ongoing customer relationships.

All customer accounts are registered and maintained in the customer's sole personal name, including date of birth and address.

#### **4.1.2 Geolocation block / IP detection**

The Company does not accept registrations from its List of Prohibited Jurisdictions. This policy is managed by the Compliance department and is approved by the executive management. This list always includes all FATF blacklisted countries and heavily Sanctioned countries.

A geolocation block detects and prevents persons located in severe risk countries from registering on the site. Countries subject to such a block are detailed on the [List of Allowed and Prohibited Jurisdictions](#).

#### **4.1.3 Device detection**

The system detects the device identifier from the user upon each login. This can be used to detect multiple users utilising the same device. This information is displayed in the back-office system and utilised by the Fraud and Risk team on a risk-based approach.

#### **4.1.4 Automated duplicate account prevention**

Players may only register one account per individual and to register other accounts is a breach of the terms and conditions of the relevant site.

Automated controls prevent a customer registering an additional account where duplicate identifier details are present.

Duplicate account controls are subject to continuous technical development to counter the typologies encountered.

#### **4.1.5 Manual duplicate account detection (III.1 – AML regulations)**

New registrations are monitored by the Fraud and Payments team daily in accordance with their departmental procedures. In the event of any obvious fictitious account creations, the account will be immediately closed. If there is doubt in relation to the customer's identity or any other registration information furnished, then customer due diligence document verification will be sought.

Additionally, the registration system does not allow anonymous or numbered accounts.

#### **4.2 PEP and Sanction screening**

The company utilizes [W2 FullCircI](#) to screen customer details against a large volume of data sources including PEP registers and extensive financial sanction lists. The data source lists are retained by the compliance officer.

Customers are immediately screened upon their first deposit to site and on a monthly screening cycle thereafter.

All screening results are manually reviewed by the Fraud and Payment team and where applicable guidance is sought from the compliance officer.

The detection of a confirmed PEP status results in a mandatory High customer risk rating, notwithstanding the relationship is immediately closed.

Individuals whose name is included in any recognized financial sanction lists, including the UN, the EU, and Curacao, shall not be accepted as customers. Where a customer is accepted and subsequently appears within a sanctions list, the account will immediately be blocked, and an internal report will be completed and escalated to the compliance officer for consideration of any external reporting requirements.

### 4.3 Verification Documents

Verification documents should be requested in the following situations unless valid documents are already held on the customer's account: -

- Potential matches from PEP, Sanction, and adverse media screening results and the provision of documents would assist in making a determination;
- In the event of any unusual account activity;
- When the customer has carried out financial transactions of NAF4,000 or greater (lifetime deposits and withdrawals);
- If the customer is assessed as a high risk;
- In the event of suspected money laundering and/or terrorist financing – where guidance should first be sought from the compliance officer.

#### 4.3.1 Acceptable ID and POA

To verify a customer's identity, the following documents are generally acceptable where they contain a photograph and are valid: -

- Passport;
- National identity card;
- Residency permit;
- Driving licence.

To verify a customer's address, the following documents are generally acceptable when they are dated within the last 6 months:-

- Bank or credit card statement;
- Local authority rates bill;
- Utility bill;
- Mobile phone bills;
- For customers resident in Switzerland – a copy of correspondence or statement from a Swiss Health Insurer (*this is on the basis that health insurance is compulsory in Switzerland and requires the data subject to hold a valid Swiss National ID card*).

Once verification documents are requested, customers are immediately prevented from making any withdrawals until suitable documentation is received.

### 4.4 Payments

The Company currently accepts four categories of payment types from customers – namely debit and credit cards, prepaid cards/vouchers, eWallets and Cryptocurrencies.

Withdrawals can be made to debit and credit cards, eWallets, Cryptocurrencies, and bank transfers. Bank transfers account for most withdrawals. All bank withdrawals are sent to a bank account beneficiary name pre-populated to match the gaming account name.

Each payment instrument has its own inherent risks and control measures in place.

#### **4.4.1 Cryptocurrency**

The company offers customers the ability to utilise certain CVC's to transfer to our PSP, before they are converted into fiat currency and utilised for gameplay. All customers' deposits and gameplay are in fiat currency.

The company is cognizant of the inherent risks associated with CVC's and acknowledges that it can never be certain of the identity of an owner of a CVC wallet and acts on a commensurate risk-based approach to mitigate these risks. This outlines the Company stance and controls specific to cryptocurrency transactions to mitigate the risk of illicit financial transactions being made on site.

The PSP utilizes a blockchain data analysis provider, to carry out crypto transaction monitoring for AML/CFT and Sanctions compliance. All deposits and withdrawal requests are screened for the following indicators and factors (list not exhaustive):

- Identification of severe-risk parties including Sanctions lists, child abuse material related entities, and terrorist financing;
- Alerts for specific behavioral patterns;
- Continuous monitoring for every registered transaction, automatically alerting changes and developments in either blockchain analysis providers data or user's transaction history.

In the event a wallet sending a depositing transaction to the Company is assessed as a high risk by the blockchain analysis provider, then the transaction is pending and manually reviewed by the PSP. If the exposure is direct (i.e., from the immediate transferring wallet), the transaction is stopped.

If the exposure is indirect, a risk-based approach is taken with a decision made to either stop the transaction or allow it to proceed.

Deposits and withdrawals flagged as a severe risk are not processed by the PSP. The provider is subject to SAR reporting requirements and reports of suspicions where locally licensed.

The Compliance team has a line of contact with the PSP's Risk Team in case of need.

Whilst all account activity should be considered on its merit, the following crypto activity may indicate potential concern and warrant further investigation (this list is not exhaustive): -

- Crypto deposits made but funds attempted to be withdrawn without gameplay;
- Crypto deposits made but funds not utilised for gameplay for a significant period of time;
- Crypto deposits which are significantly greater in value and/or frequency when compared to the typical account activity;
- Customer indicates that the crypto wallet concerned in the transaction belongs to a

third party;

- Transactions rated a high or severe risk by Cryptopay.

In the event of any unusual activity, the account is deactivated while it is reviewed. Information and/or documentation may be requested such as obtaining a transactional screenshot of the crypto payer so that a specific crypto transaction can be matched.

In the event of the knowledge of or suspicion of ML/TF/PF is present, then an internal Suspicious Activity Report is submitted to Compliance.

On a risk-based approach, the following blocking and freezing options are available and can be applied on a customer's account in relation to their crypto use: -

- Account restriction;
- Blocking the specific use of cryptocurrencies;
- Account closure.

All records are kept in accordance with Curacao law.

#### **4.4.2 Proof of Deposit**

On a risk-based approach the Company will obtain payment verification. This requirement could take place at any stage of the customer lifecycle but will typically take place whilst handling service requests, transaction monitoring and upon risk-based events.

#### **4.5 Ongoing Monitoring (III.2.4 – AML regulations)**

The Fraud and Payments team is responsible for the ongoing monitoring of customer accounts, in accordance with their departmental procedures. This includes ensuring that all customer documents stored remain valid and up to date throughout the client-business relationship.

##### **4.5.1 Transaction monitoring**

Transaction monitoring involves scrutinising transactions in conjunction with the account activity to ensure they are consistent with our knowledge of the customer.

The Fraud and Payments team carry out daily risk reports which are subject to refinement and enhancement in consideration of the trends and typologies encountered. Examples include risk reports identifying first time depositors, new registrations which appear to have links to existing accounts, manual assessment of withdrawal requests, and casino integrity checks in relation to large winners (*list not exhaustive*).

##### **4.5.2 Risk based events**

Customer account reviews take place upon any risk-based events such as expiry of documents, name changes, change of address, and or any inconsistencies or concerns.

## 4.6 Enhanced due diligence (III.4 – AML regulations)

Enhanced due diligence is additional measures that must be carried out in addition to standard customer due diligence for higher risk customers, in the event of unusual activity or in the event of suspicious activity.

Customers who have provided acceptable EDD information or documentation — or for whom the company has independently located such information — will have the back-office checkbox "**EDD Approved**" selected for tracking purposes. In addition, the EDD information or documentation is uploaded to the customer's document file.



### 4.6.1 Triggers for enhanced due diligence

EDD information is always required in any of the following circumstances:-

- Where a customer poses a high risk of ML/FT as assessed by their customer risk assessment;
- In the event of any unusual activity;
- In the event of any suspicious activity - where direction should be obtained from the compliance officer;
- Residents of high-risk countries.

### 4.6.2 Enhanced due diligence requirements

Enhanced due diligence ("EDD") can be tailored to each customer depending on the information known and risks posed.

It always includes taking reasonable measures to establish the source of wealth ("SOW") of the customer.

SOW is the origin of a person's financial standing or accumulated total net worth. It is the activities or circumstances which have generated a person's financial funds or assets. This is typically accumulated from the customers' employment, in the form of a regular salary, but sometimes maybe from other sources such as long-term investments or an inheritance.

By understanding a customer's source of wealth, we are improving our knowledge of our customers' financial position and thereby obtaining assurance that their financial activity on our site is legitimate.

EDD may also include the consideration as to whether:

- Additional identification documentation needs to be obtained;

- Undertaking further research of the customers profile is necessary, such as open-source checks;
- Additional ongoing monitoring of the customer is required.

#### **4.6.3 Failure to meet EDD requirements and termination of the business relationship (III.8)**

If EDD requirements are not met within a reasonable timeframe, the customer's account is restricted to prevent any further activity. Reinstatement of such accounts can only be considered upon meeting the above-mentioned requirements.

During the process, if the failure to complete the process gives grounds to know or suspect the customer of a ML/TF/PF offence, then an internal must be submitted to the compliance officer without delay and the client's account blocked. A record of all attempts to obtain any necessary information and documentation is recorded in the back-office journal notes.

## **SECTION 5 – RISK ASSESSMENTS**

A risk-based approach is taken when determining the appropriate levels of due diligence required, ongoing monitoring and any other restrictions placed on customers. Broadly, ML/FT/PF risks posed can be broken down into the following areas:

### **5.1 Business Risk Assessment (II.2.1 – AML regulations)**

The Company must carry out an assessment that estimates the risk of ML/FT/PF posed by the business and its customers.

The assessment is documented and reviewed annually or earlier in the event of a significant business change. Updates to version and approval history are recorded. The BRA is created and maintained by the compliance officer and is approved by the Board.

The BRA has regard to all relevant risk factors including the nature, scale and complexity of the Company's activities; the findings of the most recent Curacao National Risk Assessment and, where appropriate, the National Risk Assessment of any other jurisdictions of significance; the products and services provided; the manner in which the products and services are provided; and the involvement of any third parties for elements of the customer due diligence process.

### **5.2 Technical developments risk assessment (II.2.3 – AML regulations)**

The Company must also carry out an assessment that estimates the risk of ML/FT/PF posed by any technology utilised by the business.

The assessment is documented and reviewed annually or earlier in the event of a significant business change. Updates to version and approval history are recorded. The TRA is created and maintained by the compliance officer and is approved by the Board.

The TRA has regard to all relevant risk factors including the technology used to comply with AML/CFT legislation and shall be updated under the following conditions when:

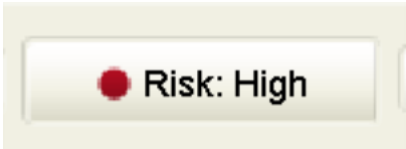
- a new product is developed;
- a new business practice emerges;
- a new delivery mechanism becomes available;
- a new or developing technology is used for both new and pre-existing products.

**5.3 Customer Risk Assessment (II.2.2 – AML regulations)**

The customer risk assessment (“CRA”) helps support the Company’s efforts in appropriately mitigating AML/CFT/PF risks and help ensure the safety and security of the platform and its users.

Implementing effective risk assessment measures helps identify potential high-risk customers for review so where necessary those risks can be appropriately managed, in line with a risk-based approach.

Customers are assigned a low-risk score upon successfully registration to the site with their activity and scoring under continuous assessment thereafter. Customers are graded either low, medium, or high with the scoring visible on the back office.



The risk scoring system allows a risk reason category and comments. When the risk score is determined, both the existing score and the new score are populated in the customers journal notes together with the date, operator, and reason.

|                                 |                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Risklevel                       | High                                                                                                                         |
| Risk Reason                     | Other                                                                                                                        |
| Other Reason                    | Politically Exposed Person (PEP)<br>High-Risk Country (including FATF 'A' List)<br>Sanctions<br>Adverse Information<br>Other |
| <input type="text" value="Q-"/> |                                                                                                                              |

Customers assigned a high risk are subject to an enhanced level of oversight.

**5.3.1 High Risk factors**

Any of the following risk factors result in the customer being rated a high risk:-

- A customer that is resident or located in a FATF [List A Jurisdiction](#) is deemed a mandatory high-risk customer;
- Any customer that is the subject of a warning in relation to AML/CFT/PF matters which is issued by a competent authority is deemed a mandatory high risk;
- Any customer who has a designated PEP status notwithstanding that the company policy is to offboard any customers who hold this status upon detection;
- Any customer who is sanctioned by a recognized financial sanctions regime including the UN, EU, and any list published by Curacao.

### **5.3.2 Geographical risk factors (11.2.3.2 – AML regulations)**

The company maintains a [List of Allowed and Prohibited jurisdictions](#) under the Curacao license. This policy is managed by the Compliance department and is approved by the executive management.

This list always includes all FATF blacklisted countries (List A) and heavily Sanctioned countries and these countries are subject to geolocation IP blocking.

In the event the Company identifies that a person is a national/resident to a country that is considered as non-reputable (or has links to such), such customer accounts shall be reviewed with consideration as to whether the relationship should be continued, or any mitigating measures are required.

IP mismatches are assessed by the Fraud and Payments team within daily risk reports and during risk-based events such as withdrawals.

IP address is also assessed during high value withdrawal requests where account registration IP and current location IP are compared, and any mismatches, including card mismatches, are investigated. Where doubts exist, information and/or documentation is requested from the customer so that an understanding of the mismatch is established.

## **SECTION 6 – RECORD KEEPING (IV.3 – AML regulations)**

This section details the obligations of the company and its staff to ensure records are kept in accordance with the legislation and standards of good business practice.

### **6.1 Identity Records**

Details of the Customers' full name, residential address, date of birth and any other relevant identification information and documentation that may have been obtained by the Company will be securely held within the back office.

## **6.2 Transaction Records**

The company will maintain records of all Customer accounts and their relevant transactions sufficient to identify the source and recipient of any payment or receipt of funds.

## **6.3 Record retention**

All transactional records will be held for a minimum of 5 years from the date when either:

- The party concerned ceases to be a customer of the Company;
- The last transaction was carried out for the customer.

In the event an external disclosure has been made to the FIU, there is knowledge that a matter is under investigation by a competent authority, or there is an awareness that a request for information from a competent authority is underway, then all relevant records must be retained as long as required by the competent authority.

## **SECTION 7 – INTERNAL & EXTERNAL REPORTING PROCEDURES**

As a business operating in the regulated sector, we have a legal requirement to report activity where we have knowledge or suspicion of money laundering, terrorist financing or proliferation financing. Failing to disclose such matters is a serious criminal offence. The term 'money laundering' includes where we know or suspect criminal funds have been deposited on our site irrespective as to whether those funds have been won, lost, or subsequently withdrawn.

### **7.1 Compliance officer (V.3 – AML regulations)**

The company shall formally designate a senior officer at management level and independent from the games operations, responsible for the detection and deterrence of money laundering and terrorist financing. The AML/CFT compliance officer must have timely access to customer identification data and other COD information, transaction records, and other relevant information. The compliance officer must be able to act independently. The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and

accuracy with other sources;

- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions as necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

## **7.2 Potential Suspicious Events (red flags)**

During the customer relationship, there may be circumstances identified as unusual or of a concern. The following circumstances would normally be a trigger that warrants further investigation with consideration as to whether a SAR report should be made:-

- Unusually large bets against the customers history;
- Customer deposits significant sums with no game play;
- Unusual deposit patterns against the customers' profile;
- Deposit methods alter on a regular basis with no rationale;
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the customer's wealth;
- Customer provides fake or deliberately misleading documents;
- Customer attempts to register multiple accounts;
- A customer requests information regarding how to conceal transactions from government authorities, especially the tax authorities;
- Transactions in the amount of NAf. 5,000 or more;
- Clients who deposit funds from bank accounts in non-reputable jurisdictions or request to withdraw funds to such jurisdictions;
- The specific red flags related to Proliferation Financing, as addressed in Point 2.4.

## **7.3 Internal Reports (IV.1 – AML regulations)**

It is important that staff understand their individual obligations to submit internal SAR's to the compliance officer within 7 days of suspicion.

If, during the course of the day-to-day operation of customer's accounts, a staff member feels that any activity is suspicious he or she must:

- Report any suspicions of money laundering, terrorist financing or proliferation financing in relation to an activity or transaction (including attempted activity or transaction that has been turned away) to the compliance officer in the prescribed format (see [Appendix 2](#));

- Ensure that the report contains sufficient information and detail outlining the nature of the knowledge or suspicion;
- Submit all other relevant evidential information and documentation referenced in the report to the compliance officer;
- All documentation making up the report shall be legible and contain sufficient information to enable the compliance officer to understand the contents and determine contraventions of AML/CFT/PF legislation;
- Note that the failure to report suspected or actual knowledge of money laundering or terrorist financing is a criminal offence;
- Note that it is an offence to disclose information to any person that is likely to prejudice an investigation.

It may be appropriate for the compliance officer to instruct staff to contact the customer to clarify certain activities and/or request additional supporting documentation. We should never 'tip off' or tell the customer that a report has been made or contemplated as this is a criminal offence. We should simply advise that the account is subject to a routine review, if restricted, or if applicable a business decision has been made to close the account.

The compliance officer's responsibilities are:

- To acknowledge receipt of the SAR from the staff member and log the same in the *Suspicious Activity Reports Register*;
- To review the SAR and the information contained within it to determine whether the information in the report supports the suspicion or knowledge and if there is a need to file a disclosure with the Curacao FIU;
- To ensure that they have full access to all systems, files and any other document or process required to fully investigate and evaluate each report;
- To record decisions made regarding a SAR received, conclusions reached and whether or not a disclosure is filed with the FIU;
- To submit a disclosure to the relevant external authority if they feel that any further explanation/documentation provided is insufficient to eradicate any reported suspicion.

#### **7.4 Whistleblowing and Confidentiality**

Whistleblowing is a key component of the Company's AML/CFT/PF program. It enables employees and other relevant parties to raise concerns about suspected illegalities, including money laundering, terrorist financing, breaches of financial sanctions, or other serious financial crimes, in a safe and confidential manner. Whistleblowing plays a critical role in identifying and

preventing financial crime and supports regulatory authorities in enforcing financial laws and regulations.

Reports are reviewed by the Compliance Officer, the appointed Whistleblowing Officer, via the compliance email (compliance@bluepepperbv.com), who assesses the nature of the concern and determines whether an investigation is required. All whistleblowing reports are formally acknowledged within a reasonable timeframe.

Any investigation will be conducted promptly, thoroughly, and impartially, with appropriate steps taken to establish the facts and assess potential breaches of laws, regulations, or internal policies. Where appropriate and permitted by law, the whistleblower will be informed of the outcome of the investigation and any actions taken. Records relating to whistleblowing reports, investigations, and resulting actions are maintained confidentially in accordance with applicable record-keeping and data protection requirements.

Where a whistleblower reasonably believes that their concern has not been adequately addressed internally, they may escalate the matter to the appropriate external regulatory or supervisory authority, in line with applicable laws and regulations.

All whistleblowing disclosures will be treated with the utmost confidentiality. Information will only be shared on a need-to-know basis for the purposes of investigation or where disclosure is required by law or regulation. The Company is committed to protecting the identity of whistleblowers wherever possible and is committed to supporting individuals who raise concerns in good faith. Whistleblowers will be protected from any issues that may be caused as a result of making a report. Appropriate support will be made available throughout the process, including access to counselling or other support services where required.

## **7.5 Register of money laundering, financing of terrorism and proliferation financing reports**

The compliance officer maintains a register detailing any disclosures made to the FIU, relating to suspicions of money laundering, terrorist financing or proliferation financing. The register will contain details of the date of the enquiry, the name of the person making the report, any relevant identification references, and a date of acknowledgement of receipt of the relevant report by the FIU.

### **7.5.1 External reports (IV.1 – AML regulations)**

Unusual transactions identified must be reported to the Curacao FIU without delay, together with any other suspicious activity or breaches identified.

Once a disclosure has been made to the Curacao FIU the company are required to hold on to the relevant identification documents and customer account records for an indefinite period. These documents will be held separately and retained indefinitely until such a time that we are authorised by the FIU to destroy them.

## **SECTION 8 – STAFF, TRAINING AND MONITORING COMPLIANCE (V.4 – AML regulations)**

This section provides the expectations for the company to ensure that staff employed have the necessary experience and expertise to fulfil their responsibilities and duties under their contract of employment. The screening process also aids in preventing criminal and fraudulent activity occurring internally. All staff must adhere to the highest levels of integrity and honesty as would be expected in the course of their employment.

The company takes reasonable and practical measures to ensure that all staff understand their obligations to fulfil their duties under AML/CFT legislation.

It is incumbent on staff to ensure that they act honestly and with the integrity expected by the standards of good practice. Staff shall ensure that they understand their obligations under this manual and where necessary seek guidance from senior management or compliance staff.

### **8.1 New staff appointments**

The [Staff Vetting Policy](#) serves as the core framework for conducting appropriate checks to ensure that all new employees and potential candidates are deemed suitable before being entrusted with responsibilities within the organisation. By implementing a sound vetting process, the business aims to maintain a safe and secure working environment, protect the interests of customers and stakeholders, and uphold the values and reputation of the business.

The owner of this policy, and all actions listed within it, is the HR department.

### **8.2 Staff Training**

The [Compliance Training Policy](#) outlines the framework established by the company for promoting internal compliance awareness and education among its staff.

The objective is to cultivate a culture of adherence to regulatory requirements and internal policies and foster a comprehensive understanding of AML/CFT requirements. Training is provided to all directors, senior management, and appropriate employees.

Violation of these laws and regulations are subject to administrative and criminal sanctions.

#### **8.2.1 Compliance Academy**

The [iGaming Academy](#) is an online training platform which is administered by the Compliance team.

Training is assigned to all relevant employees and covers courses including Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation Financing and Curacao AML regulations.

AML training is issued shortly after employees join the business and thereafter on an annual basis.

The Academy features a robust reporting centre which allows the Compliance team to gather completion records as required, whilst also providing the score achieved.

A member from the Compliance team reviews all staff training records monthly, to ensure that all courses have been completed. Those who do not complete the training are emailed to remind them that completing their training is a regulatory obligation. If training has not been completed after the initial reminder, the head of Compliance is informed of the individuals who have not yet completed their training and are personally contacted to investigate further.

### **8.2.2 Compliance Knowledge Hub**

The [Compliance Knowledge Hub](#) is a dedicated space for all compliance related information, providing a valuable resource for staff.

The Hub is a repository for Compliance and AML related policies, regulations, and information and plays a pivotal role in helping foster a culture of compliance.

### **8.2.3 Ad hoc and bespoke training**

To further enhance our commitment to continuous learning, ad hoc training is provided particularly where there are new business developments or new legislations which may have a bearing on AML/CFT.

Records of any AML related ad hoc training are recorded by compliance.

## **8.3 Testing of the AML program (V.5 - AML regulations)**

The AML compliance program must be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit must be independent, thus performed by people not involved with the organization's AML compliance staff. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable. These tests must include at least:

- An evaluation of the institution's anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;

- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The audit team should also consider whether the board was responsive to earlier audit findings. The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or the Board of Supervisory Directors, and to the designated officers with a request to take prompt corrective actions by a certain deadline. These corrective actions could also include enhancements of controls and procedures. Such corrective actions will typically be required to be implemented and reported back to the Board within 30 days or as prescribed by the Board.

#### **8.4 Examination by the Gaming Control Board (V.6 - AML regulations)**

All casinos shall provide information or documentation on their money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year. The casino shall make the following items readily available:

- a. Its written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation;
- b. Records of its Business Risk assessment;
- c. The name of each Compliance Officer responsible for the casino's overall money laundering and terrorist financing policies and procedures and his/her designated job description;
- d. Records of reported unusual transactions;
- e. Records of unusual transactions which required closer investigations;
- f. Records of frozen accounts;
- g. Schedule of the training provided to the casino's personnel regarding money laundering, terrorist financing and proliferation of weapons;
- h. The assessment report on the casino's policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor;
- i. The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

## **SECTION 9 – APPENDICES**

### **9.1 Appendix 1 – Politically Exposed Persons (III.6 – AML regulations)**

#### **9.1.1 Politically Exposed Person**

A Politically Exposed Person ("PEP") is an individual who has a high-ranking job in a government or other type of political position and therefore possesses a certain form of political influence. Family members and close business associates of the individual are also considered a PEP under

Curacao legislation.

PEPs are considered high risk because they are more likely exposed to opportunities to accept bribes and be involved in corruption due to their position.

The Company does not provide services to any customer who has the PEP status and will exit the relationship upon detection.

### **9.1.2 PEP definition according to Annex 1 of the AML regulations**

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, Judicial or military officials, senior executives of state-owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

### **9.2 Appendix 2 – SAR Internal Reporting Form**

A copy of the SAR internal reporting form is available from the [Compliance Hub](#) where guidance information is also available. When completed, the form should be submitted to the compliance officer by email.

### **9.3 – Appendix 3 – Curacao Financial Intelligence Unit Online Reporting System**

To view and obtain access to the FIU's goAML online reporting system you should use the link below.

However, only registered compliance staff should access the system.

[https://portal.fiucuracao.cw/goAMLWeb\\_PRD/Account/LogOn](https://portal.fiucuracao.cw/goAMLWeb_PRD/Account/LogOn)

