

Customer Acceptance Policy

GB Tech Services N.V

Document Information

Subject	Customer Acceptance Policy
Purpose	GB TECH SERVICES N.V policy for acceptance of customers
Involvements	All departments
Responsibility	Director
Approval	Director
Review	Annually or earlier as needed
Classification	Company Confidential

Change History

Date	Ver.	Author	Summary Changes	MLRO
	1.0	GB TECH SERVICES N.V	New Customer Acceptance policy document created as part of AML/CFT Program review	Philip Bugeja

Contents

Contents.....2

1. Introduction.....3

2. Customer Acceptance Policy3

 Aims of customer acceptance.....3

 Identity.....3

 Geographical limitations.....4

 Higher risk categories of clients.....4

 Responsible gaming4

 Ongoing monitoring.....4

 Termination4

References.....5

1. Introduction

Based on the requirements of various statutory obligations, and the Prevention of Money Laundering Act¹, GB TECH SERVICES N.V. ("the Company") has taken a position on who they can and cannot accept as a customer.

In general, the Company would not like to turn away genuine customers as the business requires acceptance of as many customers as possible to generate revenues. However, due to various local and international laws and regulations, not all customers willing to have an account with the company are able to do so.

The company will operate using a medium conservative approach, with a risk appetite that will be balanced in order to ensure compliance with all applicable obligations and to maintain a safe customer base whose higher risk portion is controlled and monitored intensively.

2. Customer Acceptance Policy

Aims of customer acceptance

- i. The Company shall only accept customers with intentions to avail themselves of remote betting services and shall not establish relationships with individual persons who would not have such intentions.

Identity

- ii. The Company does not open accounts or deal with customers of unknown identity or who have fictitious or unreal names.
- iii. The Company will only accept customers who are at least eighteen years old or have reached the age of maturity as established in the customer's country of residence, whichever is the highest.
- iv. The Company will identify and verify the customer's identity and origin in accordance with the extant anti-money laundering legislation in force in Curacao, as may from time-to-time be updated and/or revised, which are reflected in the company's Customer Due Diligence Procedures. The Company will also meet the requirements derived from any other applicable laws and regulations within the timeframes set within, where applicable.
- v. The Company will try its best not allow any registration or activity from customers who utilise any technological measure to misrepresent or obfuscate their geographical location or origin. In times of swift technological advances, the

company will keep its systems updated to be able to face the threats applicable to the industry.

- vi. The Company shall not accept customers acting on behalf of third parties and may terminate the business relationship if at any time the company has reason to believe that a customer's account is being used by third parties.

Geographical limitations

- vii. Persons who originate from countries that are considered as being a High Risk of Money Laundering or Financing Terrorism activities, as regularly highlighted by the Financial Action Task Force ("FATF"), and the Caribbean Financial Action Task Force ("CFATF") shall not be accepted as customers of the Company. If in doubt the MLRO is to be requested to provide the latest country risk assessment.

Higher risk categories of clients

- viii. Politically Exposed Persons ("PEPs") shall not be accepted as customers by the Company unless specific Senior Management approval is obtained, and enhanced due diligence is carried out. Such customers shall be specifically flagged, and ongoing enhanced monitoring of the account shall be carried out.
- ix. Individuals whose name is included in any Financial Sanction Lists compiled by the United Nations and/or the European Union shall not be accepted as customers. Individuals whose name is included into such lists after they would have been accepted as customers will have their account closed. Ongoing checking of active customers against such lists must be carried out.
- x. The Company will not enter relationships with individuals that have been identified or suspected to have committed acts of fraud or bonus abuse with other operators. The Company will also not engage in, or continue, business relationships with individuals who are identified to have been involved, suspected of or known to be associates of individuals involved in criminal activities.
- xi. The company will ensure higher risk customers are reviewed on an ongoing basis to monitor the risk in the relationship.
- xii. The Company will carry out all relative checks pertaining to PEPs, sanctions, and Negative Media ("NM") through the checking system "Dilisence".

Responsible gaming

- xiii. The Company will not enter relationships with individuals who have self-excluded, temporarily or permanently or indicated in any way that they might suffer from responsible gaming issues.

Ongoing monitoring

- xiv. The Company does not risk assess clients only at registration stage. Rather, customer acceptance may be reviewed at any time in a customer's relationship with the company, whether active or not, in order to protect the company's interests and compliance with the applicable obligations.

Termination

- xv. The Company may decide at any time to stop its relationship with a client, subject to due process and management authorisation where abruptly ending relationships may cause a criminal to be made aware of investigations occurring in relation to the client's account.

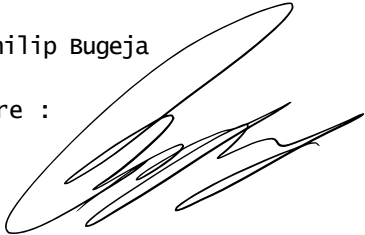
References

FATF – www.fatf-gafi.org - Improving Global AML/CFT Compliance: On-going Process – 19th October 2018

United Nations - [Financial Sanctions Consolidated List](#)

MLRO: Philip Bugeja

Signature :

A handwritten signature in black ink, appearing to be 'Philip Bugeja', written over a large, light grey oval watermark.

11/10/2024

Anti-Money Laundering and Countering Financing of Terrorism Policy

GB TECH SERVICES N.V

Document Information

Subject	Anti-Money Laundering and Countering Financing of Terrorism Policy
Purpose	GB Tech Services N.V's Policy document containing policies to comply with AML Legislative and Regulatory requirements.
Involvements	All departments
Responsibility	Money Laundering Reporting Officer
Approval	Directors
Review	Annually or earlier as needed
Classification	Company Confidential

Change history

Date	Ver.	Author	Summary Changes	MLRO
	1.0	GB TECH SERVICES N.V	New document created as part of AML/CFT Program review	

Contents

Contents	3
1. Introduction.....	4
2. Scope of this policy.....	4
3. Money Laundering Reporting Officer	5
4. Risk Assessment	5
4.1 Business ML/FT Risk.....	5
4.2 Customer ML/FT Risk	6
5. PEP / Sanctions Lists Checks	6
6. Customer Due Diligence	6
7. Payment Methods	7
8. Suspicious Transaction Report	7
9. Notifications of Fraud and Law Enforcement or Regulatory Authorities' requests	8
10. Employee training	8
11. Employee screening	8
12. Retention of Records	9
Appendix 1. References	10
Appendix 2. Glossary of Terms.....	11

1. Introduction

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

The Proceeds of Crime are funds derived from illicit sources and from which a benefit or enjoyment may be obtained. Although the aim is not to launder the funds or to fund terrorism it is still considered to be an illegal activity and subject persons should be aware of such activity and must report it as if it was ML/FT.

The policies set forth herein (the “Policies”) are intended to satisfy the statutory requirements of the relevant legislation and to provide direction to GB TECH SERVICES N.V (or the “Company”) in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism.

The Company is aware that criminals and terrorists may attempt to use the Company’s services to channel funds from illegal activities.

The National Ordinance on the Reporting of Unusual Transactions (NORUT) provides indicators to help identify unusual transactions. These indicators (consisting of objective and subjective indicators) describe when an (executed or intended) transaction is to be labeled as unusual, and thus should be reported to the pertinent national authorities.

Objective Indicator: In this case, the reporting entity is obliged to report an unusual transaction. The list of objective indicators describes under which circumstances a transaction is to be considered as unusual. Objective indicators may include the following:

- A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
- An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance;
- A transaction giving cause to assume that it may be connected with money laundering or terrorist financing.
- A transaction amounting to NAF (ANG) 5,000.00 or more, regardless whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner;
 1. A giro-based transaction amounting to NAF (ANG) 5,000.00 or more: A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank account carried out at the request of the client addressed to the service provider.
 2. The taking into deposit or the releasing out of deposit of an amount of NAF(ANG) 5,000.00 or more, at the request of the client.
 3. Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more. The term "tokens" includes at least chips and credits.

4. Payout of prizes in the amount of NAF (ANG) 5.000.00 or more. 5. All other cases

Subjective Indicator: In case of a subjective indicator, the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, their gaming (-related) activity and any other circumstance that may be relevant) has reasonable knowledge to presume that a transaction is related to money laundering or terrorism financing. In case the answer to this assessment is yes, then the reporting entity has the obligation to report.

2. Scope of this policy

The scope of this policy is to establish policies from which procedures on internal control, risk assessment, risk management and compliance in relation to AML/CFT will be drawn up.

Users of this and related policies should also refer, where relevant, to the new Penal Code of Curacao, relative National Ordinances, and Ministerial Decrees, measures/guidelines which may be issued from time to time by any relevant authority or agency.

Unless the context requires otherwise, words and expressions used in the Policy shall have the same meaning as that set out in the applicable laws and regulations.

The Company is determined and committed to prevent the carrying out of financial activities through its systems that may be related to AML/CFT.

The Company shall comply with its obligations at law by establishing the necessary and relevant processes to prevent AML/CFT and to ensure any suspicious activities are escalated to the relevant authorities.

The Policies outline the general and minimum standards of internal anti-money laundering and combating funding of terrorism (AML/CFT) which should be adhered to by the Company's management and employees.

3. Money Laundering Reporting Officer

A Money Laundering Reporting Officer (MLRO) is appointed to be the business owner of AML/CFT Risk Assessment, Controls, Policies and Procedures the MLRO shall be VJOLLCA MURATAJ.

The MLRO appointed should possess professional experience, training and resources to carry out his/her appointment as per regulations.

The MLRO answers directly to the **Board of Directors**

The MLRO responsibilities shall include but are not limited to:

- (a) risk assessment and management;
- (b) ensuring customer due diligence measures and ongoing monitoring;
- (c) record-keeping;
- (d) promoting internal control;
- (e) perform internal auditing of AML/CFT processes (unless internal auditing function is available);
- (f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures;
- (g) monitoring of relevant staff and agent screening;
- (h) Self-education and education of relevant staff in AML/CFT on an annual basis or more regularly if deemed necessary;
- (i) liaison with law enforcement authorities; and
- (j) manage Investigation Order requests received from the authorities.

4. Risk Assessment

4.1 Business ML/FT Risk

The company is to carry out a yearly risk assessment to:

- Identify ML/FT Vulnerabilities;
- Identify ML/FT Threats; and
- Identify any new requirements.

Based on the results of the Business ML/FT Risk Assessment and if deemed necessary, in order to minimise any new risks identified or existing risks being re-classified, the following controls would need to be revisited and amended accordingly:

- Measures;
- Policies;
- Controls; and
- Procedures.

The Business ML/FT Risk Assessment should also be updated whenever substantial changes to the Company's systems, processes and overall operations are carried out.

The Business ML/FT Risk Assessment and related measures, policies, controls and procedures are to be recorded and made readily available for review by interested authorities at any time.

4.2 Customer ML/FT Risk

Customers are to undergo an ongoing ML/FT Risk Assessment from the start of the business relationship and thereafter based on:

- customer type;
- products used (e.g. sportsbook);
- services (e.g. poker, bingo, betting exchange);
- transactions/payment systems;
- delivery channels; and
- geographical origin of the customer and/or payment method.

After registration, a customer's activity will undergo ongoing monitoring through automatic and manual processes to reconsider risk level depending on changes in customer's activity and to establish the point of reaching the relevant due diligence requirements thresholds.

5. PEP / Sanctions Lists Checks

Customers are also to be screened to confirm that they are not included on Sanctions Lists. Customers are asked on first deposit to confirm whether the customer is him/herself, or is a family member of, or known associate to, a person that is considered a Politically Exposed Person ("PEP"). The customer is further checked to confirm PEP status once the relevant thresholds are hit, or the customer's profile is considered to be higher than low risk.

Customers matching any one of these categories are to be automatically considered as a high-risk profile and appropriate measures taken to ensure that the business activity with them is not of an ML/FT nature. Sanctioned individuals cannot be accepted as customers. Refer to **PEP / Sanctions Lists Procedure** and **Customer Acceptance Policy**. PEP and Sanctions List checks will be carried out against the software "Sanction Check and PEP screening".

It is the reporting entity's responsibility to perform ongoing checks of its client database against the international lists of designated persons/ entities/ groups to make sure the reporting entity is not permitting/ facilitating access to funds to the ones mentioned on the sanctions lists. The primary sanctions list reporting entities must check against are UN, EU, USA-OFAC lists, Curacao National Lists (currently not in place), local lists of all jurisdictions where online gaming and gambling activities are provided and/or clients are accepted.

Instances of sanctions screening:

- during initial client/player registration;
- with every play instance;
- daily;
- with every payout/cashout.

6. Customer Due Diligence

Customer Due Diligence (CDD) Measures include:

- collection of identification details;
- verifying the Identity of the Customer;
- determining the customer profile and levels of activity and adjusting the profile as and when necessary;
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the results of the risk assessment; and
- retention of records of these checks and update them when there are changes.

The Customer Due Diligence Procedure defines the procedure used to carry out Customer Due Diligence including timeframes when this will be triggered and in which cases Enhanced Due Diligence will need to be performed.

Depending on the customer's risk profile, customers who have been requested to complete the CDD Procedure may have their account restricted during this period.

Should the CDD Procedure not be completed within the established timeframes of such a request, the customer's account will be considered to have failed completing CDD and thus will be denied from any further activity. The raising of a Suspicious Transaction Report ("STR") is to be considered. Such a decision is to be taken and recorded by the MLRO.

Unless a STR has been raised and an appropriate period has passed in which the customer has still not completed CDD, the account may be closed, and deposited funds still present on the customer's account will be returned to the deposit method, where possible, less any charges incurred by the business for transmission to this destination.

7. Payment Methods

The company will not accept to receive or make cash deposits or payments in relation to customer's activities.

The company will only make use of payment methods that are:

- Offered by licensed financial institutions and regulated by an European Economic Area ("EEA") financial regulator; and

The Company will hold received payments from customers into a player's account, distinct from Company accounts.

The Company will always keep track of transactions carried out using these payment methods and identify funds that are received or remitted by customers, together with any transfers of funds that are made into or out of the player's account for settling the customer's remote gaming activity. It will also be able to identify when thresholds for due diligence have been reached.

In all instances, where possible, funds returned to customers shall be returned to the customer's originating payment method. If this is not possible due to the nature of the payment method or in case of the account not being available any more to receive funds, payments will be transferred only to a bank account in the customer's name, following completion of the customers' due diligence process.

Transaction monitoring will be carried out through the use of internal systems and controls.

8. Suspicious Transaction Report

An internal Suspicious Transaction Report is to be sent directly to the MLRO whenever there is a suspicion that a customer is engaged in ML/FT.

No one is to divulge to co-workers, line managers and especially the customer/s that an STR has been raised as this is potentially considered to be 'tipping-off'. An employee who raises an STR must escalate directly to the MLRO.

Refer to the Internal Suspicious Transaction Report Procedure for guidance on STR escalation.

9. Notifications of Fraud and Law Enforcement or Regulatory Authorities' requests

The Company will record and take appropriate actions whenever a notification of fraud or requests by Law Enforcement or relevant Regulatory Authorities are received. The Company will follow a due process to ensure such notifications or requests are processed without delay and the Company will, within its abilities, to assist such authorities effectively.

Notifications, Law Enforcement and Regulatory authorities' notifications may also provide just cause to ensure the company's Responsible Gambling, Fraud, Money Laundering and Terrorist Funding risk mitigation strategies are working effectively. Where gaps are identified, the Company will take immediate action to resolve such gaps.

All reports should be sent without delay to the FIU. The term "without delay" is interpreted as follows:

1. Regarding Objective Reports (Reports based on an objective indicator): With the exception of the Banking Sector all reporting entities should send their unusual transaction reports within 48 hours after the transaction has been executed, or after there has been an intention for a transaction.
2. Regarding Subjective Reports (Reports based on a subjective indicator): For all reporting entities, including the Banking Sector, the time period between the execution of the transaction (or the intention to execute a transaction) and the moment the Compliance Officer receives the report, should not exceed 24 hours. As of the moment that the Compliance Officer receives the transaction report, the Compliance Officer will have 10 working days to complete the relevant research with regards to a possible Money Laundering/Terrorism Financing (ML/TF) situation. If after the research period (maximum 10 working days), there is a suspicion of ML/TF, the Compliance Officer must report the transaction within 48 hours to the FIU.

10. Employee training

Within an appropriate period of the commencement of employment, employees are to be provided with ML/FT training to ensure they are aware of measures, policies, controls and procedures that are in force. This training shall include:

- General awareness of Money Laundering / Terrorism Funding for all employees
- Specific Guidance on the related measures, controls, policies and procedures in place within the company for employees specifically occupying roles related to AML/CFT Controls and Compliance
- An assessment to ensure that the employee has grasped the key points of training received.

The training provided to employees is to be recorded and refreshed at least annually.

The MLRO is also required to attend annual refresher training and to keep up to date with the subject.

Further information about employee training may be found in the Human Resources' relevant policies and procedures

11. Employee screening

The Company's prospective employees that are to be involved with or connected to activities that would fall within the scope of this policy, are to be screened before they are employed. The Company is to ensure that they are fit and proper to occupy positions in which they will participate in the provision of services to the customer. The use of third party screening providers may be engaged to ensure this.

The Company will carry out monitoring of the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the company's operations and obligations. The Company will at all times do its utmost to respect the privacy of its employees.

Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the MLRO and / or Directors directly and should they wish to remain anonymous, to do this via an anonymous letter or email service providing as much facts and information as possible.

Further information about employee screening may be found in the Human Resources' relevant policies and procedures.

12. Retention of Records

Customer and Transactional data collected during the relationship with the customer will be maintained for a period of five (5) years from the ending or termination of the customer relationship. End of the customer relationship is defined as from the last day the customer effected any movement of funds to and from his account, or a successful login.

Should statutory obligations arising from other laws, regulations or based on a request from a regulator, a requirement be established to keep records for a longer period be in place, this will be taken in consideration and adhered to.

Documents will not be retained beyond the required obligations and will be deleted.

Appendix 1. References

United Nations - [Financial Sanctions Consolidated List](#)

European Union – [Consolidated list of sanctions](#)

MLRO: **Philip Bugeja**

Signature :

A handwritten signature in black ink, appearing to be 'Philip Bugeja', written over a light blue horizontal line.

11/10/2024

Appendix 2. Glossary of Terms

AML – Anti Money Laundering

CDD – Customer Due Diligence

CFT – Combatting Funding of Terrorism

EDD – Enhanced Due Diligence

DE – Designated Employee

FATF – Financial Action Task Force (www.fatf-gafi.org)

MLRO- Money Laundering Reporting Officer

PEP – Politically Exposed Persons

RBA – Risk Based Approach

SAR – Suspicious Activity Report

SDD – Simplified Due Diligence

STR – Suspicious Transaction Report

Sanction and PEP Screening Procedure

GB TECH SERVICES N.V

Document Information

Subject	Sanction and PEP Screening Procedure
Purpose	GB TECH SERVICES N.V Sanction and PEP Screening Procedures to comply with AML Legislative and Regulatory requirements.
Involvements	All departments
Responsibility	Director
Approval	Director
Review	Annually or earlier as needed
Classification	Company Confidential

Change History

Date	Ver.	Author	Summary Changes	MLRO
	1.0	GB TECH SERVICES N.V	New Sanction and PEP Screening Procedure created as part of AML/CFT Program review	

Contents

- Contents 3
- 1. Financial Sanction and PEP screening Procedure 4
- 2. Definitions 5
 - 2.1 PEPs..... 5
 - 2.2 Financial Sanctions..... 7
- 3. Risk-based approach 7
- 4. Strategy for Mitigating Risks..... 7
- 5. Screening process..... 8
 - 5.1 Financial Sanctions..... 8
 - 5.2 Politically Exposed Persons 9
- Appendix 1. PEP/SL monitoring system 10
- Appendix 2. Template to Sanctions Monitoring Board 11
- Appendix 3. References 12

1. Financial Sanction and PEP screening Procedure

The purpose of this document is to set out GB Tech Services N.V (“the Company”) procedure to screen new and existing customers for Financial Sanctions (FS) and Politically Exposed Persons (PEP).

Furthermore, it is at the Company’s discretion whether to accept PEPs as per the Customer Acceptance Policy.

2. Definitions

2.1 PEPs

There is no single definition of a PEP, however the definition typically consists of the following five layers:

1. Current or former senior official in the executive, legislative, administrative, military, or judicial branch of a government (elected or not)
2. A senior executive of a government-owned commercial enterprise, and/or being a corporation, business or other entity formed by or for the benefit of any such individual
3. Any individual publicly known (or actually known by the relevant institution) to be a close personal or professional associate
4. A senior official of a major foreign political party
5. An immediate family member of such individual; meaning spouse, parents, siblings, children, and spouse's parents or siblings¹.

¹ <https://pep-caribbean.com/faqs>

2.2 Financial Sanctions

From time to time the United Nations, European Union, the Financial Action Task Force (FATF) and other Governmental Authorities issue Financial Sanctions (FS) against companies, countries and individuals. The Financial Sanctions vary in type and severity and there could be stiff penalties and punishment for non-compliance with the measures requested to be imposed.

There are multiple Financial Sanctions lists available and these are to be used to assist in ensuring new and existing customers do not appear on them. Unlike PEPs, persons on sanction lists cannot be accepted or kept as customers.

Any person on a sanction list who attempts to become a customer must be blocked and that person reported to the MLRO.

Such persons must, without exception, be reported to the Sanctions Monitoring Board by the MLRO.

3. Risk-based approach

The Company shall follow a risk-based approach in implementing the provisions of this procedure. Employees and other personnel involved in the operation of the Company's business are expected to identify, assess and understand the ML/FT risks to which the company may be exposed and to take the measures commensurate to those risks to mitigate them effectively.

When assessing ML/FT risks, the relevant persons should analyse and seek to understand how the ML/FT risks they identify may affect the Company.

The risk posed by a specific customer may be the result of several varying factors. A differentiated approach is adopted that considers the risks an individual PEP poses based on an assessment of:

- the prominent public functions the PEP holds;
- the nature of the proposed business relationship; and,
- any other relevant factors the company has considered in its risk assessment.

4. Strategy for Mitigating Risks

In mitigating potential ML/FT risks, the company shall adopt the following strategy:

- Enhanced Due Diligence (EDD) measures for onboarding or retention of customers who are PEPs – checks on whether a client falls under the definition of a PEP, or has sanctions imposed shall be carried out through the system "Sanction Check and PEP Screening".

- continuous evaluation of customers and transaction risks;

- ongoing management and monitoring of customer accounts to identify any existing customers falling within scope of this procedure;
- adequate record-keeping of all evidence gathered of relationship and transactional activity to assist in any criminal investigations arising, and
- detection of potential ML/FT activities through ongoing monitoring of high risk accounts, through the use of the system “Sanction Check and PEP Screening”.

5. Screening process

- In order to check further for customer-based risks, the Company manually runs the data of newly depositing customers across industry recognised and global third-party sanctions, PEP and adverse media screening databases and those issued by the United Nations and the European Union. To this effect, the Company utilizes the system named “Sanction Check and PEP Screening”.

The system in use and the databases against which checks are made may vary from time to time, depending on outsourced partners chosen to provide the service. For this purpose, **Appendix 1** contains information about the screening system provider together with further detail about how the monitoring is carried out

Further checks may be made using open sources and if any adverse information is found, this will be considered as part of the customer’s risk assessment.

A customer’s PEP status will also be checked at significant events in the customer’s relationship with the company, such as when obliged to carry out Customer Due Diligence due to depositing thresholds as listed in the Customer Due Diligence Procedures, large withdrawals and any identified potentially suspicious activity.

5.1 Financial Sanctions

The Business will direct its financial sanctions checks against the European Union Consolidated list of sanctions¹ at the end of the registration process before the account is activated to be able to effect deposits, withdrawals or gaming transactions. In the long term, a customer is manually re-checked at significant events in the customer’s relationship with the company or on an annual basis for active customers within the preceding six (6) months. To this effect, the Company utilizes the system named “internal systems and controls”.

Should a customer be flagged as potentially being a person listed on a financial sanction list, the customer’s account shall immediately be blocked and closed. Internal escalation of such a registration is to be made to the Money Laundering Reporting Officer (MLRO) using the Internal Suspicious Transaction Report (STR) Procedure.

¹ https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions

Once the appropriate investigation is carried out, and it is confirmed that the customer is indeed likely to be a person subject to financial sanctions, a report will be submitted by the MLRO to the appropriate authority (Sanctions Monitoring Board²) to report the actions taken in respect of the customer.

Such a report may also request further guidance regarding any funds held within the customer's account. A draft template is attached in Appendix 2.

5.2 Politically Exposed Persons

Should a customer be identified at any point to be a current PEP or of having been a PEP within the previous year, the customer should be considered as posing a higher risk to the company and should hence be subjected to Enhanced Due Diligence (EDD) as described in the Customer Due Diligence Procedures.

Additional checks conducted on PEPs must include obtaining detailed information about the PEP's business or influencing power status attributed to this individual and their source of wealth. To this effect, the Company utilizes the system named "Sanction check and PEP Screening".

Approval by Senior Management, including the MLRO must be obtained prior to accepting a PEP as a customer or deciding to retain a current customer who is identified to be a PEP and if this is granted, ongoing risk monitoring must be maintained by adding the customer to the "High Risk Client Monitoring Spreadsheet" as in the "AML-CFT, Fraud and Payment Procedures".

Management approval must be given in writing and include any specific monitoring activities and conditions under which the PEP relationship has been accepted;

Appendix 1. PEP/SL monitoring system

Ongoing PEP/SL Monitoring System in use	"Sanction check and PEP Screening".
Application	
Timing & Frequency of Checks	<i>Example:</i> - At registration for PEP / SL / Adverse Media - Scans for new Financial Sanctions Targets done on inclusion in lists - Manually triggered for ANG 3856.28 in deposits over previous 180 days if last check was carried out more than 180 days ago. - May be checked manually through web interface, must be done for each deposit/withdrawal above ANG 28922.07. - At minimum once yearly for active customers within preceding 270 days.
Databases used in checks	- United Nations Consolidated List - European Union Consolidated List of Sanctions - Office of Foreign Assets Control (OFAC) – USA - Consolidated List of Financial Sanctions Targets in the UK - UK
System in operation since	IN PROGRESS
Internal support contact	www.goplay365.com
Provider Support contact	www.goplay365.com
Any other information	

Appendix 2. Template to Sanctions Monitoring Board

Dear Sirs/ Madam,

Whilst scanning our customer database for persons subject to International Sanctions, we have identified a customer profile that we are considering to be matching to a person profile in one of the International Sanctions Lists that we scan our customer database against.

We have taken the steps to immediately disable the account and have not been in communication with the customer. Should the customer get in touch, we will only request Enhanced Due Diligence information and documentation, but we will not reactivate the account unless it transpires that the person involved is not the sanctioned person, or, upon due authorisation from your end.

Customer Data:

Data Field:	Contents:
Customer Registered Full Name:	John Paul SMITH
Customer Date of Birth:	01/05/65
Address:	12, Long Road, Johannesburg, South Africa, 12344

The Customer account was immediately closed as it provided a near 100% positive hit with the UN Sanctions List, based on his name and date of birth. Within the UN Sanctions List, the address above appears to differ very slightly.

The Customer held no funds in his account at the time it was closed down.

We kindly solicit confirmation of the receipt of this notification and request further guidance to be able to meet all legislative requirements.

Appendix 3. References

United Nations - [Financial Sanctions Consolidated List](#)

European Union – [Consolidated list of sanctions](#)

MLRO: **Philip Bugeja**

Signature :

11/10/2024

A handwritten signature in black ink, appearing to be 'Philip Bugeja', written over a light blue horizontal line.

Customer Due Diligence Procedures

GB TECH SERVICES N.V

Document Information

Subject	Customer Due Diligence Procedures
Purpose	GB TECH SERVICES N.V procedures to verify customers
Involvements	All departments
Responsibility	Director
Approval	Director
Review	Annually or earlier as needed
Classification	Company Confidential

Change History

Date	Ver.	Author	Summary Changes	MLRO
	1.0	GB TECH SERVICES N.V	New Customer Due Diligence Procedures document created as part of AML/CFT Program review	Philip Bugeja

Contents

- Contents3
- 1. Introduction - baseline customer profile.....4
 - Baseline Customer Profile as seen in a low-risk customer:4
- 2. Simplified Due Diligence6
- 3. Customer Due Diligence6
- 4. Enhanced Due Diligence7
- 5. Due Diligence Sanctions9
- 6. Long term due diligence records updating.....9
- 7. Records Keeping10
- Appendix 1. Further reference.....11
- Appendix 2. Establishing SoW at CDD level11
- Appendix 3. Due Diligence Process map12

1. Introduction - baseline customer profile

GB Tech Services N.V ("the Company") is obliged to carry out due diligence on its customers with the aim of ensuring a safe conduct of play for all other customers as well as to ensure that the Company's services are not used to participate or facilitate illegal activities such as fraud, money laundering or terrorist financing.

However, the Company also understands that most customers use the Company's services for the purpose of enjoyment and recreation without the intention to carry out any of the above-mentioned acts. In view of this, the Company strives to implement a risk-based approach to due diligence based on the Business Risk Assessment (BRA), triggered according to the customer risk assessment as described within the **AML/CFT Procedures**.

Effective completion of due diligence measures for medium or high risk assessed customers must lead to re-assessment of the customer's risk rating. It is therefore important that the following due diligence measures are followed and implemented effectively, as correct application will enable the company to understand better its customers and treat them as required.

In line with this approach, low risk-rated customers are not required to provide due diligence information, subject to them remaining within this risk assessment. Medium-risk customers are required to provide information for verification, whilst the extent of information to be requested from high-risk customers must be commensurate to the risk level.

Baseline Customer Profile as seen in a low-risk customer:

An example profile of a customer who does not need to be subjected to additional due diligence would be the following:

Age	21 – 60
Residential Country	Japan, EU / EEA states or HDI countries in the top 30 places ¹
Deposit Methods	Bank Transfer, Credit / Debit Card or EU licensed Ewallet (if Ewallet holder name can be confirmed through Ewallet provider and Ewallet service carried own due diligence)
Deposit and Withdrawal amounts	Not more than ANG 964.07 per day, not more than ANG 3856.28 over a six-month rolling period (Deposits); Withdrawals effected through payment methods following a proportionality principle.
Betting products	Non-P2P betting products (Casino games, Events betting) with wins/losses falling within a median range (not top/low 10%)

¹ <http://hdr.undp.org/en/composite/HDI>

Access to customer account	Customer access to account does not indicate suspicious trends like logging through multiple switching countries over a short period of time or many different devices/IPs over an unreasonably small number of days.
Red Flags	Customer does not exhibit any of the money laundering red flags as included within the <u>Internal Suspicious Transaction Report (STR) Procedures</u> .

2. Simplified Due Diligence

The Company initialises the first step of the due diligence procedure during registration when the identification of the customer takes place with the details requested from the client customer onboarding process.

At this stage the Company ensures that no duplicate accounts are established. This prevents formerly identified fraudulent accounts, customers with suspicious activity or customers experiencing gambling control problems from opening new customer accounts.

After registration, and periodically at key events, the customer's details will be automatically or manually checked against PEP, Financial Sanctions (FS) lists, as described above. The customer's risk assessment will be reviewed to consider the above event and information collected from these checks. More information regarding this type of screening may be found within the PEP and Sanctions Screening Procedure.

Monitoring will be conducted thereafter as per the risk assessment level allocated to the customer at that stage. If the risk assessment level goes above low risk, then simplified due diligence will not be appropriate and additional due diligence measures must be taken, on a risk-based approach.

3. Customer Due Diligence

If a customer departs from the baseline customer profile considered equivalent to a low-risk customer, or hits established threshold as indicated below, unless the activity is explained and understood, the customer will be considered as a medium risk customer. Transaction monitoring is carried out through the system "internal systems and controls", being a system that will manage transaction monitoring and KYC of the players.

In absence of any other unusual activity pushing the risk-level to medium risk, a customer's due diligence thresholds are:

- ANG 9640.69 in total deposits over a rolling six (6) month period via a low to medium risk payment method issued by a financial institution in a reputable jurisdiction, or;
- ANG 1928.14 in total deposits over a rolling six (6) month period, including amounts deposited via cash-like deposit methods and pre-paid / voucher systems whereby the owner cannot be confirmed or a mixture of such payment methods;

In such cases, the customer must undergo full Customer Due Diligence, whereby:

- nationality and place of birth must be provided by the customer or identified through documentation supplied;
- identity and address are verified through a reputable verification service which matches the customer's data to reliable databases;

or

documents are requested to verify

- **Identification** amongst which:
 - a valid unexpired passport, national or other government-issued identity card, residence card or driving licence.
- and
- **Residential Address** by obtaining one of the following documents which shows the customer's name and registered residential address:
 - any identification document listed in the paragraph above, where a clear indication of residential address is provided;
 - a recent statement or reference letter issued by a recognised credit institution;
 - a recent utility bill;
 - correspondence from a central or local government authority, department or agency;
 - an official conduct certificate;
 - any other government-issued document not mentioned above.

Documents must not be older than six (6) months.

- **Source of funds (basic)** are confirmed (e.g. Bank Statement, Copy of Card, EEA licensed E-wallet backend showing the customer's name as being the owner of the deposit method) – Note: do not store payment cards showing the full 16-digit card number or CVV. Card number should be edited if needed to show only the first 6 and last 4 digits (both for front and back of the cards) and the CVV number must be covered as well.

In the medium and upper levels of a medium-risk assessment, when a customer departs from the baseline customer profile by effecting deposits above ANG 3856.28 within a shorter period than the 180-day rolling period, the Company is to also ascertain the source of wealth by requesting:

- **Source of wealth (basic)** This can be achieved, for example, by a Declaration by customer regarding employment or Bank Statement showing customer's wealth. Further examples of data sources that can be used for Source of Wealth checks at CDD level can be found within Appendix 2; or
- **Source of wealth (advanced)** A higher degree of risk will require a higher standard of information to be collected. This will need to be in the form of a documentary evidence such as salary slips, tax returns, bank statements indicating income, company statements etc.

However, it is important to note that for a customer who simply hits the ANG 9640.69 threshold over a reasonable period, no SoW documentation needs to be collected as long as all risk indicators are low and identity, address and source of funds through non-high-risk payment methods are verified satisfactorily.

To minimise inconvenience to customers, a template email is to be sent to the customer once his deposits reach a level of ANG 3856.28 within a period of less than 6-months and CDD would not have been yet completed.

4. Enhanced Due Diligence

If a customer has been deemed to be a high-risk customer or at any stage becomes one, then Enhanced Due Diligence will need to be undertaken, comprising of:

- Obtain a second form of identity verification such as:
 - a Certified Identity document copy by a professional whose good standing can be confirmed;
 - Video Conferencing or Physical meeting with customer in which customer presents an Identification document from CDD list and it is confirmed that document is a genuine one and customer in live conferencing confirms a random electronic code sent via email or SMS;
 - Verification of customer details with a second reputable electronic database; or
 - Customer provides a selfie whilst holding an official identity document.
- establishing how the customer acquired his wealth to be satisfied that it is legitimate
 - salary income or company profit (Certified Payslip / Certified employer letter / audited accounts if self-employed)
 - sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter)
 - sale of property (Certified copy of contract of sale or letter from solicitor or estate agent)
 - inheritance (Certified copy of will including value of inheritance)
 - sale of company (Certified contracts, media articles, certified letter from accountant or solicitor)
- establishing the source of the customer's funds to be satisfied that they do not constitute the proceeds from crime. Ensure that deposits originate from payment methods issued by a licensed EEA financial institution and which do not allow anonymity by requesting copies of bank statements or account statements. In the case of cash deposits, the source of wealth must be established in relation to the customer's risk assessment.
- where possible, contact the payment method provider to confirm their confidence in the good standing of the mutual customer.
- In the case of a PEP, gain a better understanding of the customer's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship.

If the EDD controls are successful and the business has established EDD for the customer, ongoing monitoring in the business will be kept with the aim of identifying any possible suspicious transactions or activity. If perceived risks have been addressed appropriately, the risk level may be re-assessed.

5. Due Diligence Sanctions

Customers are granted a thirty (30) day period to assist in completing satisfactorily CDD or EDD requests. During this period, no withdrawals may be approved.

Depending on a customer's risk profile, other restrictions on customer account may be imposed during this period, such as:

- restrictions on using all or specific deposit / withdrawal methods, or
- restrictions on using any deposited funds for betting purposes.

Once the thirty (30) days period for completing CDD or EDD is over, and if a customer has still not completed the requirements requested then it will be considered that the customer has failed Due Diligence.

If customer is considered as a potential high risk of ML/FT, the Company is to consider raising an internal STR as in the Internal Suspicious Transaction Report Procedure. Further business would not be then carried out with the customer unless so authorised by the Curacao authorities to whom the STR is raised by the MLRO.

If the customer is not suspected or known to be potential high risk of money laundering and thus is not reported to the authorities, where possible, the customer's remaining deposits will be refunded back to the original deposit method and account would be closed.

Any return of deposits not to an original funding method will be affected only to a bank account in the customer's name and the Company will specify in the transaction description that the funds would have been remitted due to failure to complete CDD procedure.

6. Long term due diligence records updating

As part of the ongoing monitoring mandated by the Company's Risk Based Approach, updated CDD documentation may be requested from the customer.

Events triggering the need for such updating may include:

- the expiry of an Identity document;
- a change in address request by the customer or apparent address changes noticed;
- a change in financial instruments used for customer transactions;
- a change in geographical origin of access to the customer's account, or
- a re-assessment of the risk rating of the customer.

In such instances, the customer must be requested to provide the relevant documents to maintain the customer's CDD status.

In default of provision of requested documentation, customer's account may be subject to sanctions and appropriate escalations considered. The same time period to provide additional due diligence applies as per CDD requirements.

7. Records Keeping

Records of information obtained and received are to be kept within the player management system or in management file servers but duly noted in the player management system when these cannot be kept thereat. Periodical random reviews to ensure the validity of data that is still held is to be performed.

Records must be kept up to a minimum of five (5) years after the customer relationship is terminated but may be extended at the requirement of the relevant authorities if so requested or if there is any other applicable legal justification.

Record keeping in relation to customer due diligence will comprise the following:

- Electronic or Physical Copies of Documents provided;
- Results of Electronic Verification service;
- Communication with the customer in text, images, audio or video format;
- A detailed account of all transactions effected and, or
- Management written decisions taken regarding Politically Exposed Persons having been accepted and the reasons for acceptance;

Electronic data is stored in secure storage systems with immediate access ability controlled through pre-assigned granular access control privileges and full back up and disaster recovery facilities to ensure that no customer data is unavailable unless this is not held anymore due to retention policies.

Employees are reminded that this data may only be used for the reasons it has been collected, that is for regulatory compliance to licensing obligations and for no other purposes.

Once the period of obligatory retention requirements expires, the data, in any stored format, is to be disposed of in a secure manner as per industry best practice to ensure adequate data protection.

Appendix 1. Further reference

When trying to establish the SoW for a customer that has reached the CDD level, the following information sources may be referred to. These may be considered depending on the risk posed by the customer but not be relied on exclusively for higher risk at CDD level, with further guidance provided below.

Information found and obtained regarding a customer must be recorded within the customer's profile.

Potential Sources:

- Search for Employment Position from Social Media and estimated salaries for that position
- Signs of affluence or interests from social media
- Companies House website, Directorships
- Electronic Verification Providers search
- General Media / News Articles / Trade Journals
- Associations / Memberships / Politics
- Credit Check Service Providers
- Information obtained from payment method (e.g. Gold Card)
- Residential Address Value through property price sites / Environment in the residence address
- Email domain (personal business / company)
- Style of bets (Showing interest in specific sports or activities more associated with wealthy persons)
- Family Background (Wealthy family, Business owners etc.)
- Court Judgements / sentences (May provide further information on wealth)
- University or Qualifications background (Indicates profession)
- Schools attended (Private or Exclusive schools may indicate family wealth)

The below documentation from a customer can also be used to establish Source of Wealth in a reliable method for higher risk relationships at CDD or EDD level:

- Documents Bank Statement provided as a Proof of Address (potentially showing income source)
- Payslip if it was provided
- Copies of Share Certificates / Investments
- Proof of Sale of property
- Proof of Inheritance

- Proof of Company Sale
- Proof of Company Profits
- Gift (with accompanying letter) - less likely

In high risk situations, documents establishing Source of Wealth must be of a high degree, preferably certified by a professional to be a true copy of original.

Appendix 2. Due Diligence Process map

A map outlining the different steps in Due Diligence is shown on the next page.

Due Diligence Process

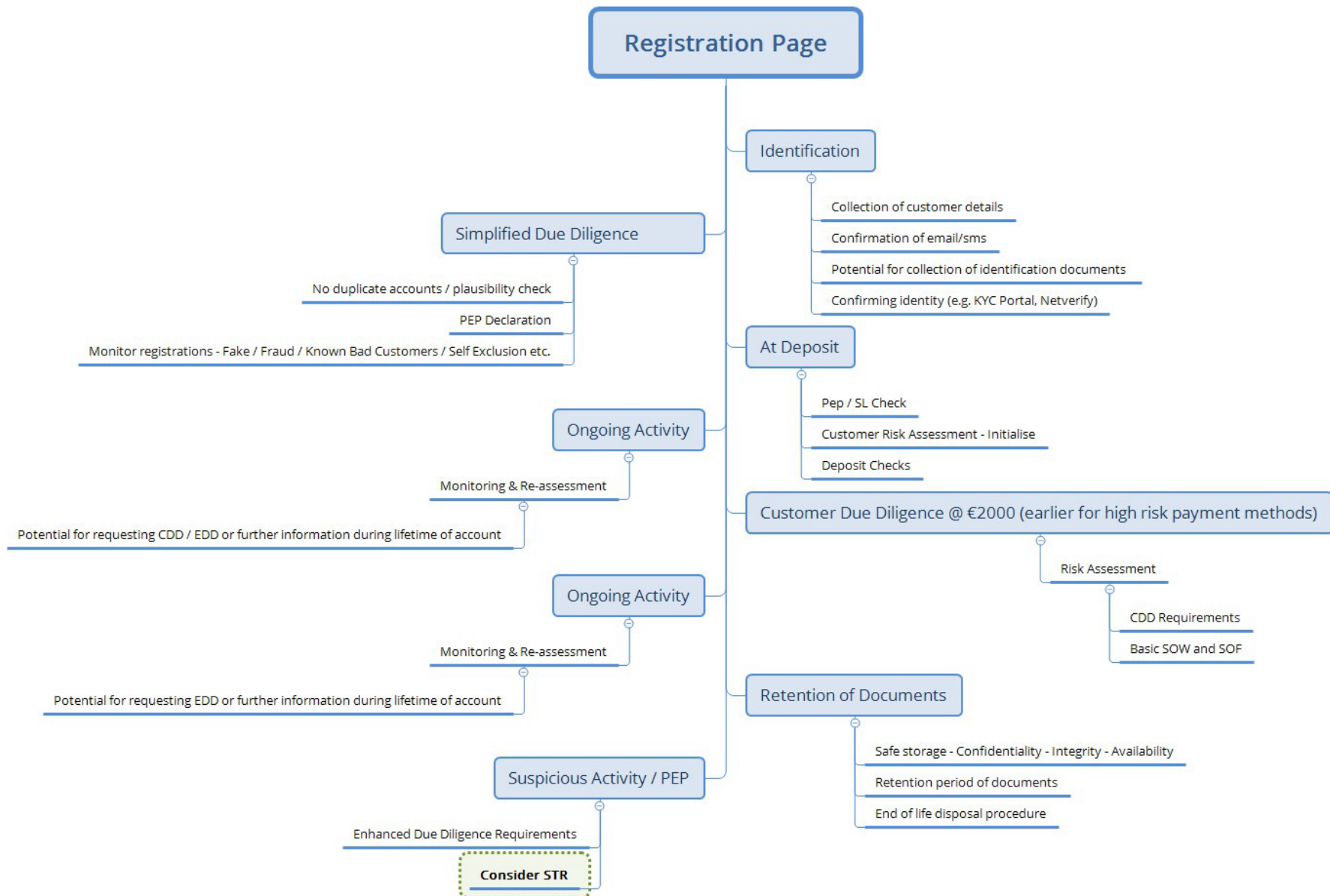


Figure 1 - Due Diligence process map

Responsible Gaming Policy

GB TECH SERVICES N.V

Company	GB TECH SERVICES N.V
Registration no.	163346
Address	Zuikertuintjeweg Z/N Landhuis Zuikertuin, Curacao
Contact	legal@goplay365.com

Document Information

Subject	Responsible Gaming Policy
Purpose	GB TECH SERVICES N.V's Policy document containing policies to implement when it comes responsible gaming and self exclusion
Involvements	All departments
Responsibility	Responsible Gaming Officer
Approval	Directors
Review	Annually or earlier as needed
Classification	company Confidential

Change history

Date	Ver.	Author	Summary Changes	MLRO
	1.0	Admin	New document created	Philip Bugeja

Contents

Contents 3

1. Policy Statement..... 4

2. General clauses 4

3. Deposit Limits 4

4. Cool Off..... 4

5. Internal Self-Exclusion 4

6. Protection of minors..... 5

1. Policy Statement

GB TECH SERVICES N.V (“the Company”) has chosen to instigate best practice policies, procedures and structures to improve its’ handling of Responsible Gaming (hereinafter this policy and procedure referred to as “RG”) Practices.

The specified policies and reporting procedures, along with the implied quality standards, apply internationally across the GB TECH SERVICES N.V group.

2. General clauses

GB TECH SERVICES N.V’s purpose is to provide entertainment in the form of a safe, secure, regulated environment. We expect our customers to use our services responsibly and in a reasonable manner. If a customer experience problems with gambling levels, there are several options available to better control the gambling habit.

3. Deposit Limits

A customer can restrict the deposit amount by setting deposit limits for a specific period of time. Separate or a combination of daily, weekly or monthly deposit limits can be set in the My Account section of the website.

Any changes to reduce or remove the deposit limits will only be applied after seven (7) days of the changes. However, if the customer chooses to decrease any limit the change will take effect immediately.

4. Cool Off

If the customer, at any point, would like to take a break for the website and suspend the use of the customer account, then the customer can request a 24 hours “cool off” period”, which is done by contacting customer support.

5. Self-Exclusion

If the customer becomes concerned about his/her gambling behaviour and wish to restrict gaming on the site, the customer can request through customer support a self-exclusion period and we will close the account upon the customer’s request. By contacting our Support team the customer can chose to have the account closed for the period

of:

- 1 month
- 3 months
- 6 months
- Permanent

If a customer chooses to be excluded permanently, the account will be terminated and any funds in the customer account will be refunded. Any changes to shorten or remove the self-exclusion period will only be applied after seven (7) days of the request.

However if the customer chooses to increase the self exclusion period it will take effect immediately.

6. Protection of minors

It is strictly against our rules for anyone under the age of 18 to engage in gambling activity or to open an account or play on our website. It is an offense for minors to participate in gambling activity.

The Website is not designed to attract children or adolescents. We are continually active in our efforts to track down and discourage minors from attempting to play on our website. We realize that the internet is a readily available resource for many, and as such, we encourage parents to take measures to contribute to the protection of their children from underage gambling.