

SEVENTIP N.V

AML & CFT POLICY



STRICTLY CONFIDENTIAL. ALL RIGHTS RESERVED.

The material contained within this document represents confidential and proprietary knowledge of WPT®Global. Any disclosure to third-party entities without the express written permission from WPT®Global is strictly prohibited. The unauthorized reproduction, storage, transmission, or any other form of dissemination of this document, whether by electronic, mechanical, photocopying, recording, or any other means, is explicitly disallowed without the prior consent of WPT®Global.

WPT®Global, all rights reserved.

STRICTLY CONFIDENTIAL. ALL RIGHTS RESERVED.

Seventip N.V – Anti-Money Laundering & Counter-Terrorist Financing Policy

Version	3.0
Effective Date	30 th May 2025
Sign Off Date	30 th May 2025
Document Owner	MLRO

VERSION CONTROL

Next Review Date	30 th May 2026
-------------------------	---------------------------

The policy will be reviewed on the following basis:

No less than once annually, with such review to be initiated by the Policy owner approximately one month prior to the date following 12 months from which the procedure was last approved.

- in response to any changes in relevant regulation and/ or legislation.
- in response to general guidance notes or best practice guidance issued by any relevant regulator.
- in response to any regulatory action taken against any operator by any relevant regulator.
- in response to findings of a relevant internal or external audit; or
- upon request of the management of Seventip N.V

NAME	ROLE
Mark Taylor	Money Laundering Reporting Officer

Table of Contents

1. Introduction	5
2. Regulatory Framework	6
3. Definition of Money Laundering and Terrorist Financing	6
4. Purpose and Scope	7
5. Customer Identification and Verification	7
6. Required Customer Information	8
7. Customer Due Diligence “CDD”	8
Due Diligence documentation	9
Personal Identification	9
Address verification	9
Source of Payment Verification	9
8. Reliance on third parties to perform CDD.	10
9. Definition of Money Laundering and Terrorist Financing	10
10. Obtaining information on the purpose and intended Nature of the Business relationship.	10
11. Transaction Monitoring and Reporting	10
12. Enhanced Due Diligence “EDD”	11
Risk-Based Approach	11
EDD Conducted	11
EDD Measures	12
Acceptable EDD Documentation	12
Training and Awareness	13
13. Ongoing Monitoring, ODD and OEDD	13
14. Counter-Terrorist Financing	14
15. Politically Exposed Persons “PEP” Screening	14
PEP Screening Threshold	14
Enhanced Due Diligence for PEPs	15
Ongoing Monitoring for PEPs:	15
Screening Systems:	15
16. High Risk Jurisdictions	16
17. Customer Specific Risk Assessment	16
Customer Specific Risk Assessment	16
Customer Risk Profile	17
Information Collection and Verification	17
18. Data Retention Policy	19
19. Suspicious Transaction Reporting (STR)	21
20. Implementation and Compliance	22
21. Training	22
22. Team Member Screening Policy	22
Regular Screening	23

Risk-Based Approach	23
Confidentiality and Compliance	23
Identity Verification	23
Criminal Record Check	23
Reference Checks	23
Qualification Verification	24
Rejection of Employment	24
Disciplinary Action	24
Reporting	24
23. AML Internal Compliance Program and External Audit	25
Regular Review:	25
Risk Assessment:	25
Team member Training:	25
Record Keeping:	25
Qualification and Independence:	26
Scope of Audit:	26
Audit Report:	26
Corrective Actions:	26
Internal Review Reports:	26
External Audit Reports:	26
Corrective Action Plans:	27
24. Due Diligence for Third parties	27
25. Policy URL	27
26. Compliance and Consequences of Non-Compliance	27
27. Contact Information	28
28. Appendix 1	29
29. Appendix 2	34

1. Introduction

1. The Anti-Money Laundering and Counter-Terrorist Financing (AML) Policy applies to Seventip N.V who will abide by the gambling license provided by the Curacao regulations.
- 1.2 This Anti-Money Laundering (AML) policy applies to the Company and all of its staff who provide services which might be used to conceal or disguise the true origins of criminally derived proceeds with the intention to make unlawful proceeds appear to have derived from legitimate origins or to constitute legitimate assets.
- 1.3 Seventip N.V are required to have adequate policies, procedures and controls that identify, assess, and mitigate the risk of Money Laundering/Terrorist Financing. This is fulfilled by implementing the following procedures and controls:
 - 1.3.1 Policies and procedures which are compliant to the regulatory requirements;
 - 1.3.2 Customer Due Diligence (CDD) is performed upon first withdrawal or at a point a customer reaches total deposits or withdrawals of 2,000 USD, further Enhanced due diligence (EDD) is only performed if considered appropriate based on the risk grading of the customer;
 - 1.3.3 An Internal and External Suspicious Transaction Reporting (STR) system; &
 - 1.3.4 Document's retention procedures.
- 1.4 Face to Face training as well as online AML Training is provided to all relevant staff at least annually.
- 1.5 Further a robust ML/TF Risk management framework is implemented across markets in order to prevent, detect and report on suspicious transactions.

2. Regulatory Framework

2. Below is a list of all the relevant AML legislation and regulations pertaining:
 - 2.1.1 Curacao Gaming Board Regulations for AML/CFT;
 - 2.1.2 National Ordinance on Identification when rendering services (N.G 2017, no 92;
 - 2.1.3 NORUT – National Ordinance on the Reporting of Unusual Transactions (N,G 2017, no 99;
 - 2.1.4 Sanctions National Ordinance (N,G 2014, no 55);
 - 2.1.5 Kingdom Sanction Act (N,G 2016, no 54);
 - 2.1.6 National Decree entering into force of Kingdom Sanction Law (N.G 2017, no 2); &
 - 2.1.7 The Code of Criminal Law (Penal Code) N.G 2011, no 48).
 - 2.1.8 National Ordinance on Games of Chance (LOK)

3. Definition of Money Laundering and Terrorist Financing

3. Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction, and confiscation of the criminal funds. There are three stages in the process:
 - 3.1.1 **Placement:** Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instrument
 - 3.1.2 **Layering:** How the link between the funds and the criminal is concealed
 - 3.1.3 **Integration:** Investing and/or recovering the funds in a way that looks legitimate.
- 3.2 As a Company policy we do not accept cash as means of payment, the Company's AML Policy is focused on preventing the use of the Company's activities and resources in the 2nd and in the 3rd stage.

4. Purpose and Scope

- 4.1 The company is mandated by the AML directives, as well as National Legislation and Regulations, to identify persons potentially carrying higher risk in order to prevent any misuse of its sites for criminal purposes. This procedure applies for all clients falling under the Curacao licence.

5. Customer Identification and Verification

- 5.1 Seventip N.V shall maintain accurate and up-to-date identification records for all customers. As part of a risk-based approach, Seventip N.V may obtain new or additional identification documents under the following circumstances:
- 5.1.1 Change in Payment Method: When a customer changes their payment method, operators should verify the authenticity of the new payment method and may request additional documentation to support the change.
 - 5.1.2 Expiration of Identity Documents: Operators must ensure that the identification documents on file are current and valid. When an identity document expires, operators should obtain a new, valid document from the customer.
 - 5.1.3 High-Risk Transactions or Behaviors: In cases where a customer engages in high-risk transactions or displays behaviors indicative of higher risk, operators should consider obtaining updated identification documents and conducting enhanced due diligence as appropriate.

6. Required Customer Information

- 6.1 The Company's KYC procedures will require prospective customers to create a full profile at the point of registration (Simplified Due Diligence). The mandatory information required at the registration stage includes.
 - 6.1.1 Full name
 - 6.1.2 Permanent residential address
 - 6.1.3 Date of birth
 - 6.1.4 Place of birth
 - 6.1.5 Nationality
 - 6.1.6 Identity number

7. Customer Due Diligence "CDD"

- 7.1 By following a risk-based approach, the appropriate due diligence can be applied to such a customer. This means that the higher the ML/FT risk is, the greater the level of due diligence will be applied.
- 7.2 The Company identifies and performs verification checks on all players, as set out by the Curacao regulations. Verification may be carried out before the customer reaches the Curacao regulations if suspicious activity is detected.
- 7.3 When a player engages in any financial transaction, whether single, series, combination, or pattern, that equals or exceeds \$2,000 USD (4,000 NAF), CDD measures must be carried out.
- 7.4 For occasional transactions that exceed the monetary equivalent of \$2,000 USD, CDD measures are mandatory.
- 7.5 If there is any suspicion of money laundering or terrorist financing activities, CDD measures must be performed regardless of the transaction amount.
- 7.6 If there are any doubts regarding the veracity or adequacy of previously obtained customer identification data, CDD measures must be reinitiated.
- 7.7 The \$2,000 USD threshold also includes peer-to-peer transfers, and CDD/KYC measures must be applied once this limit is reached.

- 7.8 Once customer due diligence is requested the customer will have 30 days to provide these documents.
- 7.9 A risk-based approach is applied in regards to obtaining up to date ID documents, when a customer is requested to provide new documents, any pending withdrawals will be held until satisfactory documents are received.

Due Diligence documentation

- 7.10 In order to verify the details on their player account, The company will request the customer to provide a copy of one document from each of the categories listed below

Personal Identification

- 7.10.1 Valid Passport
 - 7.10.2 Valid driving License
 - 7.10.3 Valid National identification Document (Picture ID)
- 7.11 Where any such document does not allow verification of one's residential address, the following documents will be requested.

Address verification

- 7.11.1 Valid National Identification Document (Picture ID) including residential address
 - 7.11.2 Utility Bill, which is less than 3 months old. Mobile phone bills are not sufficient. The bill provided must pertain to a service delivered to the address provided
 - 7.11.3 Tax Bill, which is less than 3 months old
 - 7.11.4 Copy of Bank Statement, which is less than 3 months old

Source of Payment Verification

- 7.12 When we are unable to verify the ownership of the payment method, they customer will be required to provide:
 - 7.12.1 Registered credit or debit card (Front only)
 - 7.12.2 Account statement of payment registered with the account.

- 7.13 All documents received are vetted by team members and authenticity checks ensure the documentation is genuine and have not been tampered or are fake.

8. Reliance on third parties to perform CDD.

- 8.1 The company does not rely on third parties to perform CDD measures in line with the Curacao regulatory requirements, laws and regulations.

9. Definition of Money Laundering and Terrorist Financing

- 9.1 Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction, and confiscation of the criminal funds.

10. Obtaining information on the purpose and intended Nature of the Business relationship.

- 10.1 The company will collect sufficient information to allow the detection of unusual activity in the course of a business relationship.
- 10.2 The company will either use Central statistical data to gauge the customer's activity or collect from the customer their nature of employment/business and usual annual salary upon reaching total deposits of 4000NAF/2000USD.
- 10.3 Upon request for information, the business relationship will be terminated, 30 days from the initial request to provide this information.
- 10.4 When the risk of ML/FT is higher or casinos have doubts as to the veracity of the information collected, the customer will be required to provide enhanced due diligence documentation.

11. Transaction Monitoring and Reporting

- 11.1 Any transaction or series of transactions that meets or exceeds the \$2,000 USD threshold triggers the requirement for CDD/KYC measures.

- 11.2. Upon reaching the \$2,000 USD threshold, the player will be restricted from depositing additional funds into their account or withdrawing funds from their account until the required CDD/KYC measures have been completed.
- 11.3. If the \$2,000 USD threshold is met, the business relationship with the player must be terminated within 30 days.
- 11.4. The transaction(s) must be reported to the Financial Intelligence Unit (FIU) in accordance with the regulatory requirements.

12. Enhanced Due Diligence “EDD”

Risk-Based Approach

- 12.1. Seventip N.V shall adopt a risk-based approach to Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). This approach involves identifying, assessing, and mitigating risks related to money laundering and terrorist financing based on the nature and level of risks associated with different customers, transactions, and products.

EDD Conducted

- 12.2. Enhanced Due Diligence (EDD) must be conducted in situations where the risks of money laundering or terrorist financing are deemed to be higher. Specific scenarios where EDD is mandatory include, but are not limited to:
 - 12.2.1. Residents of Higher Risk Geographic Areas: Customers residing in or transacting from regions identified as having a higher risk of money laundering or terrorist financing must be subject to EDD. This includes countries with inadequate AML/CFT regulations or those identified by international bodies such as the Financial Action Task Force (FATF).
 - 12.2.2. Politically Exposed Persons (PEPs): Customers who are Politically Exposed Persons (PEPs), including their family members and close associates, require EDD. PEPs are individuals who hold or have held prominent public positions and are at a higher risk due to their potential exposure to corruption and bribery.
 - 12.2.3. Products or Transactions that Might Favor Anonymity: Transactions or products that provide a higher level of anonymity, such as certain types of online payment

methods or virtual currencies, require EDD to mitigate the risks associated with anonymity.

- 12.2.4. New Products and New Business Practices: The introduction of new products, business practices, delivery mechanisms, or the use of new or developing technologies (both for new and pre-existing products) necessitates EDD. Operators must assess the associated risks and implement appropriate measures to mitigate them.
- 12.2.5. Unusual Transactions or Activities: Any transactions or activities that appear unusual or inconsistent with the customer's known behavior or profile must be subject to EDD. This includes large or complex transactions, patterns of transactions that are unusual, or any other activities that raise suspicion.

EDD Measures

- 12.3. In conducting EDD, operators should implement the following measures:
 - 12.3.1. Obtain Additional Information: Gather more detailed information on the customer, their source of funds, and the purpose of the transactions.
 - 12.3.2. Increased Monitoring: Increase the frequency and intensity of monitoring the customer's transactions and activities to identify any unusual or suspicious behavior.
 - 12.3.3. Senior Management Approval: Obtain approval from senior management before establishing or continuing business relationships with high-risk customers.
 - 12.3.4. Enhanced Documentation: Maintain comprehensive and detailed records of the EDD process, including the rationale for considering the customer or transaction as high risk and the measures taken to mitigate these risks.

Acceptable EDD Documentation

- 12.4. The below documentation is accepted when requesting EDD documentation:
 - 12.4.1. Payslips;
 - 12.4.2. Bank statement showing salary being received;
 - 12.4.3. Tax Return;
 - 12.4.4. Company's financials;

12.4.5. Savings.

12.5. Other types of documents may be requested depending on the person's occupation and activity on the account.

Training and Awareness

12.6. Operators must ensure that all relevant personnel are adequately trained to recognize and respond to higher-risk scenarios. Regular training programs should be conducted to keep staff informed about the latest AML/CFT regulations, risk indicators, and EDD procedures.

13. Ongoing Monitoring, ODD and OEDD

13.1. The key elements of ongoing due diligence include:

13.1.1. Regularly reviewing the customer's activities and transactions to identify any unusual or suspicious behavior.

13.1.2. Ensuring that transactions are consistent with the customer's known source of funds and expected activity.

13.1.3. Updating customer risk profiles based on ongoing transaction monitoring and any new information obtained.

13.2. Seventip N.V monitors transactions which could be related to money laundering and terrorist financing. Special attention is given to complex or unusual trends or transactions. Daily reports are received to monitor and identify unusual patterns. All reports are handled by the Fraud Team who investigate customers and if there is suspicious activity, they will escalate the matter to Seventip N.V's MLRO via the Internal SAR procedure.

13.3. Seventip N.V shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the customer, their risk profile, including where necessary the source of funds.

13.4. Seventip N.V shall ensure that documents, data, and information collected through the CDD, and EDD measures are kept up to date (ODD & OEDD).

13.5. Customers who request to amend their personal information, will be required to provide suitable documentation to verify the change in information.

- 13.6. A risk-based approach is applied in regards to obtaining up to date ID documents, when a customer is requested to provide new documents, any pending withdrawals will be held until satisfactory documents are received.
- 13.7. Customers rated as high risk and have provided enhanced due diligence documentation previously will be required to re-submit new documents every six (6) months.

14. Counter-Terrorist Financing

- 14.1. All customers are checked against the sanctions database upon initiating their first deposit, if the customer is confirmed on this list their account will be closed and an internal suspicious transaction report completed and escalated to the MLRO.
- 14.2. All customers who are re-screened are screened against the sanctions database as part of on-going monitoring.
- 14.3. Customer-facing team members are also provided with AML/CTF training during induction, as well as on an annual basis, in order to detect any suspicious activity.
- 14.4. To comply with the United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. Upon notification of a sanctioned person playing on any of the sites across the group, any funds held on the gaming account with frozen and reported to the FIU immediately

15. Politically Exposed Persons “PEP” Screening

PEP Screening Threshold

- 15.1. PEP screening must be conducted when a player's cumulative deposits reach or exceed \$2,000 USD (4,000 NAF) over their lifetime.
- 15.2. This screening helps identify individuals who may hold or have held prominent public positions and are considered to present higher risks due to their potential exposure to corruption.
- 15.3. All customers who are re-screened are screened against the PEP database as part of on-going monitoring.

- 15.4. Customer-facing team members are also provided with AML/CTF training during induction, as well as on an annual basis, in order to detect any suspicious activity.

Enhanced Due Diligence for PEPs

- 15.5. Players identified as PEPs require senior management approval to continue their business relationship with the casino.
- 15.6. Enhanced measures must be taken to establish the source of the player's wealth and the source of their funds.
- 15.7. These measures are crucial to ensure that the funds are from legitimate sources and to mitigate risks associated with corruption and other illicit activities.

Ongoing Monitoring for PEPs:

- 15.8. Players identified as PEPs require senior management approval to continue their business relationship with the casino.
- 15.9. Players identified as PEPs must be subject to increased scrutiny through ongoing monitoring.
- 15.10. The frequency of ongoing monitoring should be tailored to the risk level associated with the PEP, ensuring any suspicious activity is promptly detected and addressed.

Screening Systems:

- 15.11. Our company will implement robust systems and processes to screen all players against the specified sanctions and PEP lists during the onboarding process and on an ongoing basis.
- 15.12. Staff will be trained to understand the importance of sanctions and PEP screening, how to conduct these checks, and the necessary steps to take when a match is found.
- 15.13. Any positive matches to the sanctions or PEP lists will be documented and reported to the appropriate authorities as required by law.
- 15.14. Detailed records of all screenings and actions taken will be maintained for regulatory compliance and audit purposes.

16. High Risk Jurisdictions

- 16.1. Geographical risk assessment is conducted on all countries that the company are accepting customers, the assessment will be completed using the below lists:
 - 16.1.1. FATF Jurisdictions under Increased Monitoring
 - 16.1.2. FATF/CFATF High Risk Jurisdictions subject to a Call for Action
 - 16.1.3. EU List identifying high risk 3rd countries with strategic deficiencies
 - 16.1.4. The US Department of State Money Laundering assessment (INCSR)
 - 16.1.5. Basel AML Index
- 16.2. The company does not accept customers from high-risk countries identified on the above lists, this is enforced by blocking players from playing from these countries.
- 16.3. The company may initiate enhanced due diligence when the person's nationality, country of birth, or transactions are from countries identified by the FATF and the CFATF.

17. Customer Specific Risk Assessment

- 17.1. As part of our commitment to regulatory compliance and the prevention of financial crime, our company Seventip N.V will implement a comprehensive Customer Specific Risk Assessment process. This process is designed to evaluate the risk profile of each customer and ensure that adequate measures are taken to detect and prevent unusual or suspicious activities.

Customer Specific Risk Assessment

- 17.2. A detailed Customer Risk Assessment will be conducted for each customer at the time of account registration and continuously throughout the business relationship.
- 17.3. The assessment will consider various factors including, but not limited to, the customer's source of wealth, nature of employment, usual annual salary, and intended level of activity on the platform.

Customer Risk Profile

- 17.4. A Customer Risk Profile will be conducted for each player to gather sufficient information that allows for the detection of unusual activity throughout the business relationship. The following steps will be taken:
- 17.4.1. Collect CDD documentation and, when necessary, EDD documentation to establish the player's source of wealth and the expected level of activity.
- 17.4.2. Obtain information on the player's nature of employment or business, usual annual salary, and any other relevant financial details. When the risk is not deemed high, a declaration can be completed by the customer confirming these details.
- 17.4.3. Social media may be used as an additional source of information to validate the player's declared information.

Information Collection and Verification

- 17.5. Sufficient information and, where necessary, documentation will be collected to establish the customer's source of wealth and expected level of activity.
- 17.6. Players will be required to confirm their nature of employment or business and usual annual salary. Social media and other publicly available sources may be used to verify the information provided.

Enhanced Due Diligence for High-Risk Customers

- 17.7. Customers identified as high risk will be subject to enhanced due diligence measures. This includes obtaining additional documentation to verify the source of their funds and wealth.
- 17.8. High-risk customers must provide comprehensive documentation to support the legitimacy of their financial sources.

Ongoing Monitoring and Updating:

- 17.9. The customer risk profile will be regularly updated based on the customer's activities and any new information obtained.
- 17.10. Continuous monitoring will be conducted to detect any unusual or suspicious activities, ensuring prompt action is taken when necessary.

Compliance with Regulatory Requirements:

- 17.11. Seventip N.V will adhere to all applicable AML and CFT regulations by ensuring that customer-specific risk assessments are conducted and maintained.
- 17.12. Detailed records of all risk assessments and related documentation will be kept to demonstrate compliance during AML Audits and regulatory reviews.

Training and Awareness:

- 17.13. All relevant staff will receive training on the importance of customer-specific risk assessments, how to conduct them effectively, and the regulatory requirements associated with them.
- 17.14. Yearly training updates will be provided to ensure staff remain knowledgeable about the latest regulatory changes and best practices in risk assessment.

System Implementation

- 17.15. Seventip N.V will implement robust systems and processes to automate the collection, verification, and monitoring of customer risk profiles.
- 17.16. These systems will ensure that risk assessments are performed consistently and accurately, supporting our overall compliance efforts.

18. Data Retention Policy

Purpose

- 18.1. The purpose of this Data Retention Policy is to outline the obligations and procedures for retaining and disposing of records related to Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) activities. This ensures compliance with legal, regulatory, and operational requirements.

Scope

- 18.2. This policy applies to all records and documents obtained, generated, or maintained in connection with AML and CFT activities, including but not limited to customer identification information, transaction records, due diligence reports, and communications related to suspicious activities.

Retention Period

- 18.3. Operators are required to retain AML and CFT-related records for a minimum period of as specified by applicable laws and regulations, or for a longer period if deemed necessary based on the business's risk assessment. The standard retention periods are as follows:
- 18.3.1. Customer Identification Records: Retain for a minimum of five (5) years after the end of the business relationship with the customer.
 - 18.3.2. Transaction Records: Retain for a minimum of five (5) years from the date of the transaction.
 - 18.3.3. Due Diligence and Monitoring Records: Retain for a minimum of five (5) years from the date the due diligence or monitoring activity was conducted.
 - 18.3.4. Suspicious Activity Reports (SARs): Retain for a minimum of five (5) years from the date the report was submitted to the relevant authorities.

Storage and Security

- 18.4. All records must be stored securely to prevent unauthorized access, alteration, or destruction. This includes both physical and electronic records. Seventip N.V has implemented appropriate security measures, including encryption, access controls, to protect sensitive information.

Access and Retrieval

- 18.5. Records must be maintained in a manner that allows for timely and efficient access and retrieval. Only authorized personnel should have access to AML and CFT records, and access should be granted based on the principle of least privilege.

Disposal of Records

- 18.6. Upon the expiration of the retention period, records must be disposed of securely and in a manner that ensures the confidentiality of the information. Disposal methods may include shredding physical documents and permanently deleting electronic records. Seventip N.V shall maintain a log of disposed records, including the date of disposal and the method used.

Record Keeping

- 18.7. Seventip N.V shall maintain records, containing the information and documentation necessary to decide whether the objective of the CDD measures referred for at least five (5) years after the business relationship is ended, or after the date of the occasional transaction.

Compliance and Audit

- 18.8. Seventip N.V shall regularly review and audit their data retention practices to ensure compliance with this policy and applicable legal and regulatory requirements. Any deviations or non-compliance issues should be promptly addressed and rectified.

Policy Review and Updates

- 18.9. This Data Retention Policy should be reviewed and updated regularly to reflect changes in legal and regulatory requirements, business practices, and the risk environment. Any updates to the policy must be communicated to all relevant personnel.

19. Suspicious Transaction Reporting (STR)

- 19.1. The company has a legal responsibility to report an individual to the Curacao financial intelligence unit(s) if there is suspicion that the individual is laundering money, financing terrorist activities, or funding their gambling from the proceeds of crime.
- 19.2. If team members are in a position where they suspect that someone is laundering money or using the proceeds of crime, then they are required to report their suspicion using a predefined form called an Internal SAR and submit it to the MRLO. The internal Suspicious Money Laundering Transaction Report can be found in Appendix 1.
- 19.3. The company adheres to the stipulations of the National Ordinance for Identification of Services and to detect and report either intended or unusual transactions. Seventip N.V has implemented adequate procedures to cover:
 - 19.3.1. The recognition of unusual transactions.
 - 19.3.2. The documentation of unusual transactions
 - 19.3.3. The reporting of unusual transactions
- 19.4. Once this information has been received, the MRLO acknowledges and, as soon as practicable, reviews the information to determine if further profiling is appropriate.
- 19.5. Suspicions can also arise per investigation of an account, for example, finds adverse media or a recent criminal judgement against the player. If this is the case the customer will be reviewed by the MLRO.
- 19.6. In circumstances where the business receives an information request from law enforcement agents, the MLRO will decide whether to raise an External STR to Curacao Financial Intelligence Unit.

20. Implementation and Compliance

- 20.1. Seventip N.V is committed to complying with these new regulatory obligations to prevent money laundering and terrorist financing.
- 20.2. Staff training and system updates will be conducted to ensure that all financial transactions are monitored and that appropriate CDD/KYC measures are promptly applied.
- 20.3. Regular audits will be performed to ensure compliance with these requirements and to maintain the integrity of our operations

21. Training

- 21.1. The company will provide team members with an approved programme of training in relation to the topics and themes considered by the AML policy and procedures. Topics cover both money laundering and terrorist financing.
- 21.2. A written record will be retained of all training received by team members.
- 21.3. All team members are required to refresher training every 12 months.

22. Team Member Screening Policy

- 22.1. Seventip N.V follows high ethical standards in the recruitment of all its staff. This includes taking prospective team members' professional background into account.

Purpose

- 22.2. To ensure the integrity and security of operations, operators will establish and adhere to robust policies and procedures for screening team members for criminal records. This is a crucial part of the overall risk management strategy to prevent and detect any involvement in money laundering or terrorist financing activities.

Screening Policies and Procedures

- 22.3. Seventip N.V shall implement the following team member screening measures:
 - 22.3.1. Before hiring, all potential team members must undergo a thorough background check, including the verification of criminal records. This

screening should cover both domestic and international criminal databases to ensure comprehensive checks.

Regular Screening

22.3.2. Existing team members should be subject to periodic re-screening to identify any changes in their criminal record status. This is particularly important for team members in sensitive roles with access to customer information and financial transactions.

Risk-Based Approach

22.3.3. The level of screening should be commensurate with the risk associated with the team member's role. Higher levels of scrutiny should be applied to team members in positions with greater potential influence over AML/CFT controls, such as senior management and compliance officers.

Confidentiality and Compliance

22.3.4. All screening procedures must be conducted in compliance with applicable laws and regulations, ensuring the confidentiality and protection of team member information throughout the process.

Screening Process

22.4. The team member screening process should include the following steps:

Identity Verification

22.4.1. Confirm the identity of the prospective or current team member using reliable, independent source documents, data, or information.

Criminal Record Check

22.4.2. Conduct a comprehensive criminal record check to identify any past criminal convictions or ongoing investigations.

Reference Checks

22.4.3. Contact previous employers and references to verify the employment history and character of the prospective team member.

Qualification Verification

22.4.4. Verify the educational and professional qualifications of the team member to ensure they meet the requirements of the role.

Documentation and Record-Keeping

22.5. Operators must maintain accurate and up-to-date records of all team member screening activities. This includes documentation of the screening process, findings, and any actions taken as a result of the screening. These records should be retained for a minimum period as specified by applicable laws and regulations.

Response to Positive Findings

22.6. In the event that a team member or potential team member's screening reveals a criminal record or other concerns, operators must take appropriate actions based on the severity and relevance of the findings. This may include:

Rejection of Employment

22.6.1. For prospective team members, rejection of the employment application.

Disciplinary Action

22.6.2. For current team members, appropriate disciplinary action, which could range from additional training and monitoring to termination of employment.

Reporting

22.6.3. If the findings indicate potential involvement in money laundering or terrorist financing, the matter should be reported to the relevant authorities in accordance with established reporting procedures.

Training and Awareness

22.7. Operators must ensure that all relevant personnel are trained on the team members screening policies and procedures. Regular training sessions should be conducted to keep staff informed about the importance of team member screening in the context of AML/CFT compliance and the specific steps involved in the screening process.

23. AML Internal Compliance Program and External Audit

Purpose

- 23.1. To ensure the ongoing effectiveness and integrity of our Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) measures, an annual internal compliance review and external audit are required. These processes are essential for identifying and addressing potential weaknesses in our AML/CFT framework.

Internal Compliance Program

- 23.2. Operators must establish and maintain an internal compliance program that includes:

Regular Review:

- 23.2.1. Conduct an internal review of the AML/CFT policies, procedures, and controls at least annually to ensure they are up-to-date and effective.

Risk Assessment:

- 23.2.2. Perform regular risk assessments to identify and mitigate potential money laundering and terrorist financing risks.

Team member Training:

- 23.2.3. Ensure that all team members receive ongoing training on AML/CFT policies, procedures, and their individual responsibilities.

Record Keeping:

- 23.2.4. Maintain comprehensive records of all internal reviews, findings, and any corrective actions taken as a result of these reviews.

External Audit

- 23.3. An external audit of the AML/CFT compliance program must be conducted annually by qualified and independent auditors. The key requirements for the external audit are as follows:

Qualification and Independence:

23.3.1. The individuals or entities conducting the audit must possess the necessary qualifications, expertise, and independence to ensure that their findings and conclusions are reliable and impartial.

Scope of Audit:

23.3.2. The audit should comprehensively review the effectiveness of the AML/CFT policies, procedures, and controls. This includes evaluating the implementation of risk-based approaches, due diligence measures, transaction monitoring, and reporting mechanisms.

Audit Report:

23.3.3. Upon completion of the audit, a detailed report must be provided, outlining the findings, conclusions, and any recommendations for improvement. The audit report should be reviewed by senior management and the compliance team.

Corrective Actions:

23.3.4. Any deficiencies or areas for improvement identified in the audit report must be promptly addressed. Operators should develop and implement a corrective action plan to rectify these issues and enhance the AML/CFT framework.

Documentation and Record Keeping

23.4. Operators must maintain detailed records of all internal compliance reviews and external audits. These records should include:

Internal Review Reports:

23.4.1. Documentation of the internal review process, findings, and any corrective actions taken.

External Audit Reports:

23.4.2. Copies of the external audit reports, including findings, conclusions, and recommendations.

Corrective Action Plans:

23.4.3. Records of any corrective action plans developed and implemented in response to audit findings.

Continuous Improvement

23.5. The findings from internal reviews and external audits should be used to continuously improve the AML/CFT compliance program. Operators should regularly update their policies, procedures, and controls based on the audit recommendations and evolving regulatory requirements.

24. Due Diligence for Third parties

24.1. The company has processes in place, when applicable, to carry out due diligence upon establishing a business relationship in line with our regulatory requirements and to ensure that the company only works with reputable entities

25. Policy URL

25.1. This Policy cannot be accessed online through the company websites.

26. Compliance and Consequences of Non-Compliance

26.1. The company is obligated to to apply to all regulations covered under section 2 of the regulatory framework within this policy. Should Trent Tech Group violate these regulations, the company can be subject to disciplinary actions, legal implications, or business risks.

26.2. In situation of non-compliance, the following actions could be taken:

26.2.1. The company will be subject to regulatory fines.

26.2.2. Regulatory enforcement.

26.2.3. Respective action on particular regulations and processes.

26.2.4. License revoked.

26.2.5. Assess adequately the risk of money laundering of terrorist financing.

27. Contact Information

Any questions regarding this policy, please contact:

Name – Mark Taylor

E-mail Address – markt@diligenzagroup.com

Contact Number - +356 99911164

28. Appendix 1

Internal Suspicious Transaction Report

The following Suspicious Transaction Report is used to report any suspicious transactions that need to be forwarded to the Authorities, especially for Suspected Money Laundering and Financing of Terrorism.

The suspicious transaction report should be submitted to the MLRO via e-mail to: markt@diligenzagroup.com.

Suspicious Transaction User Report

Report Date	
--------------------	--

Part 1: Sign Up Details

User Account Number:	
Title	
First name:	
Last name:	
Address:	
Country:	
Email:	
Identity Number:	
Date of birth:	
Mobile:	
First Deposit Date:	

Part 2: Suspicious Activity Information

Date or date range of suspicious activity			
Type of suspicious activity	☐	Minimal gaming with large transactions	
	☐	Unusual use of gaming activity	
	☐	Terrorist financing	
	☐	Money Laundering	
	☐	False or conflicting identification documents	
	☐	Refusal to provide documentation	
	☐	Credit/debit card fraud	
	☒	The customer's spend is not in line with the normal profile of the customer	
	☐	Opposite Betting/Card Countering	
	☐	Politically Exposed Person	
	☐	Sanctioned Person	
	☐	Adverse Media	
Details of suspicious activity			
The user acted alone or as part of a group	☒	Alone	☐ Part of a group
If part of a group include UIDs			

How did the investigation start.	☒	Internal monitoring
	☐	Reported by the bank
	☐	Reported by E-Wallet provider
	☐	Reported by the police

	☐	Reported by the Gaming Authority
3rd Parties Informed	☒	None
	☐	Issuing card bank
	☐	E-Wallet provider
	☐	Police
	☐	Curacao Gaming Authority (MGA) / SGA

Part 3: Payment Details

Card Details		
Card End Date: (first 6 and last 4)		
Name on Card:		
Card Type:		
Card Issuer:		
Card Issuing Country:		
Total Deposited:		
Total Withdrawn:		

Bank Account Number(s):		
SWIFT Code:		
Name on Bank:		
Bank Issuer:		
Bank Issuing Country:		
Total Deposited:		
Total Withdrawn:		

E-wallet Details		
E-wallet Account Number:		
First name:		
Last name:		
Email:		
Total Deposited:		
Total Withdrawn:		

Other type of methods Details		
Account Number:		
First name:		
Last name:		
Email:		
Total Deposited:		
Total Withdrawn:		

Part 4: Deposit & Withdrawal Information

Total Deposit:	
Total Withdrawals:	

Deposit Date & Time:	Deposit Amount:
Can be provided in an Excel sheet if multiple transactions included Failed Deposits	Provide in a separate Excel

Withdrawal Date & Time:	Withdrawal Amount:
Can be provided in an Excel sheet if multiple transactions included Failed Deposits	Provide in a separate Excel

Part 5: Account Verification

Documents Requested:	☒	YES	☐	NO
If YES enter date				
Documents Received:	☐	YES	☒	NO
Identity document received:				
Address documents received:				
Proof of funding Documents received:	Provide separately			

Part 6: Account Activity

Games Played:	☐	Table Games	☐	slots	☐	Poker
----------------------	--------------------------	-------------	--------------------------	-------	--------------------------	-------

Closure Date:				
Pending Withdrawal amount:				
Closure Account Balance				
Chargeback/RFI Received:	☐	YES	☒	NO

29. Appendix 2

Form to be completed by the Money Laundering Reporting Officer upon receiving the above report from a team member.

Are there reasonable Grounds for suspicion?

Is consent required from the Financial Intelligence Unit (FIU) to any ongoing or imminent transactions which would otherwise be prohibited acts? • YES • NO

If YES, please record authorisation and “way forward” details received from the Financial Intelligence Analysis Unit
--

If there are reasonable grounds to suspect Money Laundering, but you do not intend to report the matter to the FIU, please set out below your reasons for non-disclosure

Signed _____ Dated _____

THIS REPORT SHALL BE RETAINED FOR A MINIMUM OF FIVE (5) YEARS