

TC ENTERTAINMENT N.V.

Company Number: 133780
Schout Bij Nacht Doormanweg 40, 1st floor, Curacao

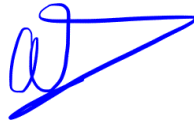
ANTI MONEY LAUNDERING POLICIES AND PROCEDURES

APPROVED BY: Andrea Engelhardt
THE MANAGING DIRECTOR OF TC ENTERTAINMENT:

eMagnus Curacao B.V.

~~XXXXXXXXXX~~
~~eMagnus B.V.~~

Date of approval:
17.03.2025



CONTENT

1. Introduction	3
2. Money Laundering Reporting Officer	4
3. Senior Management	4
4. Risk assessment	5
4.1 Risk Areas	5
4.2 Customer Risk	6
4.3 Product/ Service/Transaction Risk	7
4.4 Geographical Risk	7
4.5 Interface Risk	7
5. Customer Due Diligence	7
5.1 Identification and Verification	8
5.2 Ongoing KYC(Know Your Customer) monitoring	9
5.3 3 rd Party verification	9
5.4 Reputable Funding	9
5.5. EDD- Enhanced Due Diligence	9
6. Timing of CDD Measures	10
7. Politically Exposed Persons ("PEP")	10
8. Record keeping	11
9. Suspicious transaction reports	11
9.1 Review of Suspicious transactions	11
9.2 Procedures for reporting suspicious transactions	12
10. Application of CDD measures for existing customers	14
11. Termination of Business relationships	14
12. Audit	14
13. Prohibition of disclosure	15
14. Employees	15
15. Employee training	16
16. Enforcement	17
17. Revision and Amendments	17

1. Introduction

TC Entertainment N.V. aims to satisfy all responsibilities and requirements identified by the European Prevention of Money Laundering and Funding of Terrorism Regulations, Directive (EU) 2015/849 of the European Parliament and the Council of May 20, 2015/(the Fourth Directive) and the 5th anti-money laundering Directive (Directive (EU) 2018/843), legislation of the European Union applicable on the activities of the Company in the field of measures against money laundering and financing of terrorism.

In the preparation of the Policies and Procedures, the International Standards for the Prevention of Money Laundering and Financing of Terrorism (FAFT Recommendations), the transnational risk assessment prepared by the European Commission, the reports and the opinions of the Committee of Experts on the Evaluation of Measures against money laundering and terrorist financing - MONEYVAL, the reports and statements of the European Commission's Expert Group on Policies for the Organization and Conduct of Gambling, as well as the accepted international standards, have been taken into account and considered

The objectives of these Policies and Procedures shall be:

1. To contribute to the prevention and detection of the actions of individuals and legal entities, groups and specialized organizations of organized crime aimed at money laundering and financing of terrorism;
2. To determine the obligations of the Company as a liable person, as well as specific procedures for their implementation;
3. To establish clear criteria for identifying suspicious operations or transactions and clients related to money laundering and/or financing of terrorism;
4. To regulate the collection, processing, storage and provision of information to the Financial Intelligence Directorate of the State Agency for National Security, as well as information related to the implementation of the The Law on Measures against the Financing of Terrorism;
5. To determine the order and methods for initial and ongoing training and qualification of the employees of the Company, applying the measures against money laundering and financing of terrorism

These rules shall set out:

1. clear criteria for identifying suspicious operations or transactions and clients, participating in the gambling games organized by the Company;
2. the procedure for the use of technical means for prevention and detection of money

laundering;

3. a system for internal control over the fulfilment of the obligations established, in the regulations for its implementation and the applicable legislation of the European Union;

4. a procedure for conducting an internal audit for verification and evaluation of the rules, procedures and requirements for the proper implementation of the requirements for the prevention of money laundering and the financing of terrorism.

5. an internal system for risk assessment and risk profile determination of clients;

6. policies, control mechanisms and procedures for limiting and effectively managing the risks of money laundering and terrorist financing established at European Union level, at national level, as well as at company level, proportionate to the size and the nature of the gambling activities pursued by the Company;

7. rules and organization for the fulfilment of the obligations to clarify the origin of the funds and the source of the property status;

8. the terms and conditions for collecting, storing and disclosing information;

9. the rules for the organization and the work of the responsible employees, as well as the rules for the training of the employees;

10. the training rules for the other employees;

11. other rules, procedures and requirements according to the specifics of the gambling activity organized by the Company.

2. Money Laundering Reporting Officer

TC Entertainment N.V. appointed a Money Laundering Reporting Officer (MLRO) with sufficient seniority and command as the reporting officer.

All employees of the Company are aware of the identity of their MLRO and the deputy MLRO and how they can be contacted as well as the procedure for reporting.

Reporting officer have responsibility for:

- making reports to senior management on anti-money laundering (AML) and countering terrorist financing.
- receiving internal and external reports relating to the prevention of money laundering and countering terrorist financing.

The MLRO has the authority to act independently in carrying out their responsibilities and has access to sufficient resources to carry out the duties.

3. Senior Management

Senior management is also fully engaged in the processes around an operator's assessment of risks for money laundering and terrorist financing, and they have sufficient knowledge regarding the matter and are involved at every level of the decision making process to develop the operator's policies and processes to comply with the regulations.

4. Risk assessment

The Business Risk Assessments is carried out in order to identify the ML/FT risks the Company is exposed to and to ensure that the measures, policies, controls and procedures adopted are sufficiently robust to prevent and mitigate the same. The Business Risk Assessment is documented and approved by the Board of Directors.

TC Entertainment N.V. is using several steps in applying a risk based approach:

- Risk Mitigation – Identifying and applying measures effectively to mitigate risks
- Risk Monitoring – Putting in place management information systems and keeping up to date with changes to the risk profile through changes to the business or threats
- Documentation – Having policies and procedures to cover the above and deliver accountability from the Board and Senior Management down

The customer-specific risk assessment is carried out so that the Company is able to identify potential risks upon entering into a business relationship with a customer. This assessment enables the Company to develop a risk profile for the customer and to categorize the ML/FT risk posed by such customer as low, medium or high.

4.1 Risks Areas

- Customer Risk
- Product/Service/Transaction Risk
- Geographical Risk
- Interface Risk

4.2 Customer Risk

For the Company the customer means a natural person who seeks to form, or who has formed a business relationship with the company.

The Risk may vary in accordance with the type of the customer. The company only has natural persons as customers – the risk assessment posed by a natural person is generally based on the person's economic activity and/or source of wealth.

The risk assessment considers information held about the customer and that the information is consistent.

The information related to the client identification shall be verified by one or more of the means listed in the Rules for the Implementation of AML. The same shall be used for initial assessment of the client's risk profile.

On the basis of analysis, The Company defines a category of clients or business relationships with a higher risk, that shall be placed under special surveillance and in respect of which extended measures shall be applied.

The commercial or professional relations, operations and transactions with persons from countries that do not fully implement international standards in countering money laundering shall be subject to special supervision.

Where the operation or transaction does not have a reasonable economic justification or an apparently reasonable cause, additional information on the circumstances surrounding the operation or transaction and its purpose shall be collected as far as possible.

Widely extended measures shall be mandatory applied in relation to clients who occupy or have held a senior state positions, as well as to clients who are related to them.

The extensive measures with respect to clients may be:

1. making visits to the address specified by the client;
2. requiring additional documents and information from the client;
3. collecting information through another client;
4. online inquiries;
5. requirement of references by its counterparties in the country or abroad or by other obliged persons;
6. collection of information about the source of income;
7. verification of the client's activity, including by visiting his/her production or administrative premises or by collecting information from his counterparts;
8. check with the client's employer;
9. measures contained in instructions issued by the director of the Financial Intelligence Directorate;
10. other measures deemed appropriate.

4.3 Product/Service/Transaction Risk

Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as services that allow the customer to influence the outcome of a game, be it on his own or in collusion with others. The use by customers of specific funding methods should also be treated as high risk factors. This includes cash and other similar or anonymous payment methods that may not leave or disrupt the audit trail, and allow the

customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies. The exceptional use by a customer of accounts held or cards issued in the name of third parties is also to be regarded as a high risk factor. Conversely, where a customer transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of ML decreases – these credit or financial institutions are themselves subject persons and one would expect that as part of their CDD obligations they would monitor on an on-going basis any account or card activity.

4.4 Geographical Risk

The Company is keeping up to date with FATF reports, OFAC sanctions list, UN and EU sanction lists, media reports and country specific reports in order to keep their country risk assessments up to date.

The nationality, residence and place of birth of a customer are taken into account, since they might indicate high geographical risk.

The customers that have a connection with the countries that have a weak ML/FT system, that are on the above mentioned sanctions list, that are known to have a significant level of corruption, that have sanctions in connection to terrorism or the proliferation of weapons of mass destruction are considered high risk.

4.5 Interface Risk

The channels through which the company establishes a business relationship and/or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the same. The company adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations. The company also implemented additional measures, on a risk-sensitive basis, to sufficiently counter the above mentioned risks.

5. Customer Due Diligence

The determination of a customer's risk profile is essential to allow to apply a level of Customer Due Diligence ("CDD") commensurate to the identified ML/FT risk. CDD is intended to allow us to know who the customer is and to build a customer profile on the basis of which would be able to assess the customer's activity to identify any unusual behavior. Any such behavior has to be questioned and, if it is found to lead to a suspicion of ML/FT, it also needs to be reported to the relevant authority. The documentation and information collected will then assist the authorities in any analysis or investigation of the suspected instance of ML/FT.

Monitoring of customer behavior provides a good barometer for continual assessment of the risk posed by the customer and any deviations from what has become the norm for that individual should be identified and risk assessed.

Casinos have the obligation to undertake Customer Due Diligence measures when:

- a. players engage in financial transactions equal to or above Naf. 4,000;
- b. carrying out occasional transactions above the monetary equivalent of Naf. 4,000;

5.1 Identification and Verification

The standard identification procedure consists in the gathering of the following personal details:

- (a) name and surname;
- (b) permanent residential address;
- (c) date of birth;
- (d) place of birth;
- (e) nationality;
- (f) identity reference number where applicable.

As a rule, verification of identity has to be carried out by making reference to a government-issued documents containing photographic evidence of the customer's identity (e.g. passport, identity card, driving license etc.).

Where any such document does not allow verification of one's residential address, the Company ask instead any of the following documents which should not be more than six months old:

- a recent statement or reference letter issued by a recognized credit institution;
- a recent utility bill for a service installed and provided at a residential property;
- correspondence from a central or local government authority, department or agency;
- a record of a visit to the address by the licensee;
- an official conduct certificate;
- any other government-issued document not mentioned above; or
- the mailing of correspondence via registered mail or by means of a courier which allows us to obtain documentary evidence that the correspondence was effectively delivered at the residential address provided by the customer and signed for by the same.

5.2 Ongoing KYC (Know Your Customer) Monitoring

Ongoing KYC (Know Your Customer) policy is in place. Once a customer's identity has been verified and registration has been completed, documentary proof of identity is requested and a due diligence check is performed, at any point, based on customer activity monitoring, including:

- Frequent deposits and/or withdrawals regardless of the amount and time
- Deposits and withdrawals without the corresponding betting activity
- Unusual patterns of transactions with no apparent economic or lawful purpose
- Unusual patterns of transactions based on a specific customer's previous activity.
- Failure in velocity checks (based on frequency of change and location of IP addresses of the customer's betting/login/payments transactions and locations indicated by his/her verified documents and payment method.)
- any transaction that amounts to €2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked

TC Entertainment is also required to identify and verify the identity of the beneficial owner. As a general rule, casinos should make sure that customers are registering an account to play and transact on their behalf. This can be achieved by including specific wording in the terms and conditions that a registering player must explicitly accept, together with a declaration in the form of a tick box that a player is registering to play on his/her own behalf. Casinos are not expected to merely rely on said declaration, but have to ensure that their ongoing procedures allow for the detection of possible instances where the player is actually playing on behalf of third parties.

- It is acknowledged that in the majority of cases, casinos will not encounter situations involving beneficial owners. However, these situations cannot be excluded completely as casinos may be maintaining business relations with one or more players funded by a syndicate. In such circumstances, where the funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners and casinos would therefore have to identify them and verify their identities.

5.3 3rd Party verification

Using ID Verification/Fraud Prevention tools in order to check specific customers and verify ID documents. Some of the services offered by this tool are:

- Verifying ID cards/Driving licenses/ International Passports
- Access to Terrorist database
- Address verification
- Telephone number verification

Once 3rd party verification or manual check has verified the identity of a customer, the verification is stored on the system.

5.4 Reputable funding

Verification the first (next) payment or transaction into the customers account is carried out through an account held by the customer in his name with an authorized credit institution or recognized under the Payments Services Directive, or otherwise so authorized in another „reputable jurisdiction“. In case customers failure to complete our due diligence procedures, customer account will be terminated, and all transactions will be blocked.

5.5 EDD- Enhanced customer due diligence and enhanced ongoing monitoring

These measures are applied in the following cases:

- Customer does not cooperate in the carrying of CDD.
- Customer attempts to register more than one account.
- Customer deposits considerable amounts by means of multiple prepaid cards.
- Customer deposit funds well in excess of what is required to sustain his usual betting patterns.
- Customer makes small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patters of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquiries about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate to his wealth, known income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Threshold €2,000 reached
- in any business relationship or transaction with a customer situated in a high-risk third country identified by the European Commission
- if the operator has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP
- in any case where the operator discovers that a customer has provided false or stolen identification documentation or information and the relevant person operator proposes to continue to deal with the customer
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing
- high-value depositing customers
- dormant accounts, there is a risk that an individual may deposit funds and then not use this account for a significant period of time in the hope to distance himself from his crimes
- mismatch in country of residence/card country/bank country



6. Timing of CDD Measures

A casino provides services to a customer allowing for the wagering of a stake with monetary value in a game of chance. It does business with customers that are individuals and act in their own name and on their own behalf. In doing so it opens an account for its customers or latter becomes a member of the player club. This is considered to be indicative of a relationship that is expected to have an element of duration and therefore is considered a business relationship between the casino and its customer. For casinos, verification of identity has to be conducted when engaging in financial transactions equal to or in excess of NAf. 4,000. This implies that all CDD measures must have been conducted at the time the threshold is reached. However, casinos are required to apply a minimum level of CDD measures prior to reaching the threshold. Thus, simultaneously with the opening of an account, casinos are to identify the customer by collecting the minimum personal details, being: name and surname, permanent residential address and date of birth (set as the minimum requirements in case of low risk business relationships) and conduct the PEP status screening and sanctions screening. The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals made by the player since the establishment of the business relationship, including any peer-to-peer transfers. Once the threshold is reached, casinos have to carry out a customer risk assessment and meet their remaining CDD obligations.

Carrying out CDD as early as possible can limit situations in which a casino receives contaminated funds.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the casino obtains any necessary information from the customer concerned.

However, if the NAf. 4,000 threshold is reached because of a deposit of the player, he cannot further deposit funds into the account or withdraw funds from the account. He still will be able to play, using the funds already in his account. However, if the NAf. 4,000 threshold is reached because the customer wants to withdraw his money, a complete freezing of the account should occur. In this case it will not be possible for the customer to continue playing.

Besides that, if the requested information and documentation is not received within 30 days from the moment the NAf. 4,000 threshold was reached, the casino has to terminate the relationship with the player and report the transaction to the FIU if a presumption of money laundering or terrorist financing exists. If no presumption of money laundering exists, the funds should be transferred to the same bank account or wallet it was deposited from. If presumption of money laundering or terrorist financing exists, internal procedures should indicate whether the funds are blocked or not. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.

7. Politically Exposed Persons ("PEP")

Politically Exposed Person ("PEP") are individuals, who are or have, at any time in the preceding year, been entrusted with prominent public functions, other than middle-ranking or more junior officials, as well as to clients who are related to them

The reason that such an individual must be tracked by us is because PEP pose potential reputational risk to regulated entities.

The fact that a person is a PEP does not automatically mean that they are involved in money laundering. It is however something that could result in an alteration to their risk profile and justify enhanced customer due diligence measures being applied.

Employees in the company need to screen and identify PEPs, new customers should be screened on registration as well as regular screening of existing customers.

This include the use of internet search engines or subscriptions to suitable databases.

PEP always requires the application of EDD measures, independently of the outcome of the customer risk assessment. This entails having to determine whether a customer is a PEP or otherwise and, should this be the case, apply of the following pre-established EDD measures:

- i. Obtain senior management approval to service the PEP;
- ii. Establish what is their source of wealth and, where applicable, their source of funds;
- iii. Conduct enhanced on-going monitoring of the customer's activity. Establishing whether a person is a PEP is not straightforward and may require a number of different processes to be involved.

Additionally, the 3rd Party verification service allows for Politically Exposed Persons identification. Whether a check is automatic or manual if during verification check a customer is found to be politically exposed, the fraud team staff adds a relevant note in the customer details page, insert the user account in a PEP list and updates the MLRO.

8. Record keeping

The operator's record keeping policy and procedure covers records in the following areas:

- details of how compliance has been monitored by the nominated officer;
- tasks for the nominated officer;
- nominated officer reports to senior management;
- customer identification and verification information;
- supporting records in respect of business relationships or occasional transactions;
- employees training records;
- internal and external suspicious activity reports;
- contact between the nominated officer and law enforcement or National Crime Agency, including records connected to appropriate consent

9. Suspicious transaction reports

- All players should be screened against sanctions lists of the UN and EU. If Curaçao publishes a local
- list with designated persons and organizations, the casino should also take that local list into
- account. The casino must ensure it does not do business with customers that are subject to

- international sanctions. Before doing business or performing an occasional transaction for the first
- time with a player, the casino should check published lists of known or suspected terrorists or other
- sanctioned persons or companies through:
- UN Sanctions List <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>
- EU Sanctions List <http://www.sanctionsmap.eu/#/main;>

9.1 Review of suspicious transactions

The main responsibility of the MLRO is to consider any internal reports of unusual or suspicious transactions and, where necessary, follow up the same by filing a Suspicious Transaction Report ("STR") with the relevant authority. The MLRO is also considered by the relevant authority as its main contact point within the subject person and he is to act as the main channel through which any communications with the Authority are to be conducted.

9.2 Procedures for reporting suspicious transactions

Suspicious transactions identified by relevant departments will be reported to the MLRO, that will assess and further examine the case and keep the findings available in the Company Fraud Folder. The employees are informed and trained that the tipping off or warning a suspicious customer that the matter is being investigated is forbidden.

The MLRO will review the transactions, the customer's account history and any other relevant information and where he considers that there is sufficient evidence that money laundering may be taking place he will pass the information directly to the authorities.

The following is a list of possible red flags, usually the same ones that are already under enhanced due diligence monitoring:

- Customer does not cooperate in the carrying of CDD.
- Customer attempts to register more than one account.
- Customer deposits considerable amounts by means of multiple prepaid cards.
- Customer deposit funds well in excess of what is required to sustain his usual betting patterns.
- Customer makes small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquiries about the possibility of moving funds between accounts belonging to the same gaming group.

- Customer carries out transactions which seem to be disproportionate to his wealth, known income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- in any business relationship or transaction with a customer situated in a high-risk third country identified by the European Commission
- if the operator has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP
- in any case where the operator discovers that a customer has provided false or stolen identification documentation or information and the relevant person operator proposes to continue to deal with the customer
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing
- high-value depositing customers
- dormant accounts, there is a risk that an individual may deposit funds and then not use this account for a significant period of time in the hope to distance himself from his crimes
- mismatch in country of residence/card country/bank country

TC Entertainment N.V. has a documented process in place for all employees to report when they have suspicions that a customer may be engaged in money laundering or terrorist financing to the money laundering reporting officer (MLRO) or in his absence their Deputy MLRO.

A register will be maintained which includes the details of all enquiries made by the authorities or the reports made to the authorities.

10. Application of CDD measures to existing customers

Casinos should also apply the CDD measures to existing customers on the basis of materiality and risk and should conduct due diligence on such existing relationships at appropriate times. Casinos have to consider whether any procedures they have been applying are sufficient to meet their CDD obligations as indicated in this chapter. If this is the case, they can continue applying these and pay special attention to their on-going monitoring obligations as set out in this chapter. If a casino had no procedures in place to meet the CDD requirements, it has to apply these on a risk sensitive basis and must conduct customer due diligence on such existing relationships at appropriate times.

11. Termination of business relationship

In case the obligations arising from the customer due diligence cannot be met, TC Entertainment cannot establish the business relation or perform the transaction and is obliged to terminate the business relationship with the customer. TC Entertainment keeps a record of all the attempts made to get the necessary information and documentation. To this end, it may decide to either close the account or to keep it blocked and suspended in its entirety.

In the event that the customer makes the requested information and/or documentation available to TC Entertainment following the closure or the suspension and blocking of the gaming account, the casino has to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/TF associated with the given business relationship.

TC Entertainment considers whether there are any grounds giving rise to suspicion of ML/TF/FP. The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/TF/FP. If, the presumption of ML/TF/FP exists TC Entertainment will submit an unusual transaction report to the FIU with regard to this player.

Where there is no reason for the retention of funds, the funds are to be remitted back to the player. This has to be done through the same channels used to receive the funds.

12. Audit

Upon decision of the Company's managers, by order, a commission shall be appointed to perform an internal audit where the rules, procedures and requirements shall be verified and evaluated. The Commission must be composed of at least three people with the relevant competences.

Upon decision of the Company's managers, an independent audit and analysis may be commissioned.

For the external and internal audits carried out a report shall be drawn up, which shall be approved by the managers of the Company and shall be provided at the request of the Financial Intelligence Directorate of the State Agency for National Security.

13. Prohibition of disclosure

TC Entertainment and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. They are not permitted to disclose information to the customer nor to third parties. The reason for this is not to jeopardize an analysis or investigation into Money laundering or Terrorist financing. This is also the reason why caution is advised when a casino takes action to terminate a relationship or otherwise block additional transactions following reporting to the FIU. Drastic action should only be taken when there is no other way out, since any unjustified action may alert the player. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF. the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

14. Employees

Employees must report to MLRO officer any knowledge or suspicion of money laundering whether by customers, guests or other employees. Employees must follow TC Entertainment N.V. policies and procedures for:

- Customer due diligence, including enhanced requirements for high risk customers which includes politically exposed persons (PEPs);
- Reporting suspicious activity to the nominated officer where necessary, seeking appropriate consent to allow participation in gaming and to conduct gaming and other business transactions;
- Record keeping for those who exceed the threshold or who have a business relationship.

15. Employee training

Employees that are working directly with customers and are monitoring transactions are additionally screened before joining the team in order to ensure they haven't been related to fraud or money laundering. The screening consists of criminal history checks at the time they get hired. HR is performing reviews on a case by case basis.

New Customer Service staff, Payments Team staff and the relevant Finance staff will be trained in the accordance with the required procedures. Once new products are released training for these games will be provided to the relevant staff. These training sessions will include refresher training in anti-money laundering procedures.

TC Entertainment N.V. staff is receiving appropriate and regular training as to their responsibilities with regard to:

- customer due diligence measures
- record-keeping procedures
- internal reporting procedures
- policies and procedures on internal control, risk assessment, risk management, compliance management and communications that are adequate and appropriate to prevent the carrying out of operations that may be related to money laundering or the funding of terrorism,
- relevant regulation in each jurisdiction where a license is held;

a) New employees

A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the appropriate designated officer must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority. They shall be made aware of the existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements. They must also be trained on the money laundering methods and trends in the gambling sector. They must receive an explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions.

b) Audit staff

Those charged with overseeing, monitoring and testing money laundering controls should also be trained about changes in regulation, money laundering methods and enforcement, and their impact on the organization.

c) AML Compliance staff

These are the people who run the AML program. They will need specialized training to be able to stay on top of new trends or changes that impact the organization and the way it manages risk. This will require attending conferences or AML-specific presentations to go into greater detail.

d) Supervisors and Managers

A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.

e) Senior management and board of directors

Money laundering issues and dangers should be regularly and thoroughly communicated to the board. This to keep board members aware of the reputational risk that money laundering poses to the institution.

Refreshment training must be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends. To demonstrate compliance with aforementioned staff training guidelines, the casino shall maintain records that include:

Details on the content of the training programs;

The names of the staff members who have received the training;

The date on which the training was provided;

The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and

An ongoing training plan.

16. Enforcement

The policy applies to all officers and members of the staff, and sets out procedures for the reporting of suspected money laundering activities with the aim to reduce potential criminal activity. The policy defines procedures that will assist to comply with the legal obligations.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Companies contracted to TC Entertainment N.V. found to be violating this policy will be deemed to be in breach of contract.

17. Revision and Amendments

All TC Entertainment N.V. procedures are subject to an annual revision which has to be completed before the annual financial audit of the company. Significant changes to any policy or procedures are to be approved by the Key Officials and communicated to the Regulator.