

TORRERO PLATFORM N.V.
AML/CFT Procedure

Policy No.: AMLCFTP – v1.1
Date of Issue: 10.02.2025

Contents

1. General	3
1.1 Policy Statement	3
1.2 Definition	4
2. The Risk Based Approach	4
2.1 Definition	4
2.2 Risk Assessment	4
i. Product/Service/Transaction Risk	4
ii. Interface Risk	5
iii. Geographical Risk	5
iv. Customer Risk	5
3. Customer Due Diligence (DD)	7
3.1 B2B relationships	7
4. Reporting suspicious activity and transactions	9
4.1 Appointment of the Money Laundering Reporting Officer (MLRO)	9
4.2 Reporting suspicious activity and transactions	9
4.2.1 Internal Reporting Procedures	9
4.2.2 External Reporting Procedures	10
4.2.3 Stopping/continuing work following a suspicion	10
5. Training	11
6. Keeping records of client due diligence information	12
7. Monitoring and management of compliance	12

1. General

1.1 Policy Statement

The scope of this policy is to establish policies and procedures on internal controls, risk assessment, risk management and compliance to AML/CFT.

These policies and procedures are relevant to all employees, contractors, affiliates, or any authorized individual working on behalf of the company Torrero Platform N.V. - Curacao (OGL/2024/651/0285).

Policies and procedures set out the expectations across the above entities, however the individual processes of implementing and achieving the goals of these policies and procedures may differ due to reasons such as different back offices, software, etc.

Applicable laws and regulations governing Curacao licensed jurisdictions:

1. National Ordinance on Identification when rendering Services (N.G. 2017, no. 92);
2. National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
3. Sanctions National Ordinance (N.G. 2014, no. 55);
4. Kingdom Sanction Act (N.G. 2016, no. 54).
5. the implementation regulations of the above.
6. The implementation regulation of the Sanctions National Ordinance (in compliance with art. 10 of the NORUT and the Ministerial Regulation Indicators Unusual Transactions - N.G. 2015, no. 73);
7. the FATF- and CFATF-notifications regarding higher-risk countries (in compliance with art. 5i of the NOIS).

Unless specifically indicated phrases and expressions used in the Policy shall have the same meaning as that set out in the applicable laws and regulations.

The company is fully committed to preventing the carrying out of financial activities through its systems that may be related to AML/CFT.

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

This policy seeks to establish the general and minimum standards of internal anti money laundering and combating funding of terrorism which should be adhered to by employees at all levels.

It is the policy of Torrero Platform N.V. that all members of staff shall actively participate in preventing the services of Torrero Platform N.V. from being exploited by criminals and terrorists for money laundering purposes or used to fund a terrorist activity through winnings obtained through wagering on the company's website. This participation has as its objectives:

- ensuring Torrero Platform N.V. compliance with all applicable laws, statutory instruments of regulation, and requirements of the relevant supervisory body;
- protecting the company and all its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements;
- preserving the good name of Torrero Platform N.V. against the risk of reputational damage presented by implication in money laundering and terrorist financing activities;
- making a positive contribution to the fight against crime and terrorism.

To achieve these objectives, it is the policy of Torrero Platform N.V. that:

- every member of staff shall meet their personal obligations as appropriate to their role and position within the company;
- commercial considerations shall never be permitted to take precedence over Torrero Platform N.V. anti-money laundering commitments;

- the company shall appoint a Money Laundering Reporting Officer (MLRO), and a designate employee to ensure continuation during his / her absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointments. Any reference to MLRO in this document, will include that of the designate employee should the MLRO be temporarily absent.

1.2 Definition

Torrero Platform N.V. believes that prior to implementing its AML/CFT Policy, it is essential for it to identify what is, on the one hand, money laundering, and what, on the other hand, constitutes funding of terrorism.

Money laundering is the movement or concealment of criminal proceeds with the aim of obscuring the link between the crime and the generated funds, to be able to avail oneself of the profits of crime. Hence, the ultimate aim is that of obscuring the source of funds.

Funding of terrorism is the process of making funds or other assets available, directly, or indirectly, to terrorist groups or individual terrorists to support them in their operations. This may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organizations involved in money laundering operations. Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organization or the individual terrorist and its or his legitimate funding sources. Therefore, funding of terrorism is mostly concerned with obscuring the end recipient of the funds.

2. The Risk Based Approach

2.1 Definition

As per the applicable laws, Torrero Platform N.V. adopts a risk-based approach. It hence identifies and analyses its risks and subsequently makes use of measures, policies, controls, and procedures to curb any undesired risks, amongst which those related to the money laundering and funding of terrorism risks from materialising. The approach allows for flexibility and significant discretion to be exercised by Torrero Platform N.V. This entails significant responsibility. It is up to Torrero Platform N.V. to show via adequate documentation, including but not limited to a risk analysis process, that it has assessed all risks and adequately put into place any measures to control these risks. In this regard this policy lays out the specific steps which Torrero Platform N.V. will adopt to ensure that its conduct is in line with the Risk Based Approach in respect of considering and identifying those risks that directly impinge on money laundering and funding of terrorism.

2.2 Risk Assessment

Risk Management entails:

- i) recognition of existence of risk
- ii) undertaking of a risk assessment, and
- iii) implementing systems and strategies to manage and control the identified risks.

There is no doubt that the business of remote gaming is deemed risky. The risk assessment will however identify the key risks the company faces as well as the level of these risks, so that, consequently, the necessary measures are adopted to manage and control the identified risks. This procedure will specify the controls and processes that are to be followed to ensure that the risks which Torrero Platform N.V. has identified and which it will face as part of its operations will not materialize. Torrero Platform N.V. organizational risk assessment which is to be approved by the Board of Directors takes the following factors into consideration:

i. Product/Service Risk

This refers to the inherent risks associated with the products and services provided by Torrero Platform N.V., particularly as they pertain to money laundering and terrorism financing. As a B2B distributor of games and platform services for operators, Torrero Platform N.V. acknowledges that its products and services may be exploited by risky actors, particularly through innovative technological developments and evolving business practices. Before introducing new games or platform features from its suppliers, Torrero Platform N.V. conducts a thorough risk assessment to identify potential vulnerabilities that could be exploited for ML/TF purposes. Additionally, if new mechanisms are introduced (e.g., API-based direct operator integration, mobile app solutions), these will be assessed for vulnerabilities, such as insufficient transaction tracking or anonymity in access.

ii. Interface Risk

This refers to the channel through which Torrero Platform N.V. establishes a business relationship and/or through which transactions are carried out. Non face-to-face interactions, such as in respect of Torrero Platform N.V. business interface, are no longer considered as automatically high-risk, as long as technological measures and controls to address the heightened risk of identity fraud or impersonation are adopted. Torrero Platform N.V. will make sure to adopt a good mix of verification methods based on both documentary and electronic sources as mentioned below, so as to counter the mentioned risks. For instance, though Torrero Platform N.V. will make use of electronic databases, it is well aware that the databases only confirm that the identification details provided correspond to those of an actual person, and not that the customer is actually that individual. Provision of additional identification documents will provide further proof that Torrero Platform N.V. was justified in considering that the B2B partners is actually the person he alleges to be.

iii. Geographical Risk

This is the risk posed to Torrero Platform N.V. by the geographical location of the customers, however also the geographical locations of its suppliers and service providers. The element to be considered in respect of this AML/CFT policy is primarily attributable to the suppliers, customers and service providers, and their source of funds. The country of registration / operations of a B2B partner should be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak anti-money laundering and counterfeit terrorism system, countries known to suffer from a significant level of corruption, and countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction will be considered as high risk. The opposite is also true and hence may be considered as presenting a medium or low risk. Torrero services with use information on www.knowyourcountry.com for making a decision regarding the geographical risk of each registered customer.

Risk assessments are 'works in progress'. Such assessments are to be constantly re-evaluated as new risks emerge. Risks may emerge due to changes in technology, which may render money laundering, or the funding of terrorism attempts easier to carry out. Other changes include the widening of the customer-base or the addition of games and payment methods which present a different risk profile from those already offered, which will thus require a revision of the business risk assessment. In the absence of any such changes, Torrero Platform N.V. will re-assess its business risk assessment at least once a year, so as to evaluate whether any changes thereto are necessary. In determining the level of risk posed by a customer, the accumulation of all the relevant indicators will be taken into consideration. These together, determine the customer's risk profile contributing to the totality of a customer's risk profile.

iv. Customer Risk

This relates to the type of customer being provided with the service. In identifying the level of risk inherent in a relationship, Torrero Platform N.V. will be assessing what would be the likelihood that a customer would be able to launder proceeds of crime through Torrero Platform N.V.'s service.

Furthermore, the director & UBO of the client or supplier will be screened so as to determine whether he is a politically exposed person (PEP), or in any way associated to a PEP. Checks would also be carried out to ensure that the individual is not subject to any sanctions or other statutory measures.

2.3. Determination of the customer's risk profile

When determining the client's risk profile, it is necessary to take into account risk categories (factors) as well as circumstances that increase or decrease those risks. Torrero Platform N.V. classifies its customers into three risk tiers: low risk (tier 1), medium risk (tier 2), and high risk (tier 3).

Clients classified as low-risk (tier 1) meet the following criteria:

- The customer's risk level is low if a written long-term contract has been concluded with them.
- The customer's risk level is low if the client is a publicly listed company in a regulated market that is subject to disclosure obligations, ensuring sufficient transparency regarding the beneficial owner.
- The customer or individuals associated with them are not included in any sanctions or watchlists.
- If individuals associated with the customer do not hold citizenship in a high-risk country or a prohibited country.
- In cases where information about the client and their beneficial owner is publicly available, and the client's activities align with their everyday business operations.
- The customer has a long-established business with a solid reputation and a track record of compliance with laws and regulations.
- The customer has a stable ownership structure with identifiable and reputable shareholders or beneficial owners.
- The customer is registered in a jurisdiction with a low risk profile, not included in the list of high-risk countries.
- The customer has implemented robust internal controls, policies, and procedures to prevent money laundering, fraud, and other financial crimes.
- If individuals associated with the customer do not hold the status of a politically exposed person (PEP), the customer's risk level is categorized as medium.

Clients classified as medium-risk (tier 2) meet the following criteria:

- The customer's risk level is considered medium if information regarding the ultimate beneficial owner (UBO) is not publicly available.
- The customer's risk level is considered medium whether or not a long-term contract has been established with them.
- The customer is registered in a jurisdiction that may have moderate risk factors but is not listed as a high-risk country.
- The customer's management team has a generally positive reputation and a history of responsible business practices.
- The customer has a relatively stable ownership structure with identifiable shareholders or beneficial owners.
- The customer has a moderate likelihood of being involved in activities that may carry some risks related to money laundering, terrorism financing, or other illicit activities.
- The customer's risk level is not considered medium if they meet any criterion indicating characteristics of a higher-risk category.

Clients classified as high-risk (tier 3) meet the following criteria:

- The customer is registered in a high-risk country.
- The customer's risk level is considered high if individuals associated with them hold citizenship or residency in a high-risk country.
- The ownership structure of the corporate customer appears unusual or overly complex considering the company's operations, or it is not possible to determine the ultimate beneficial owner.
- Doubts have arisen during the identification of the person's identity or the verification of the provided information, including doubts about the accuracy of the data or the authenticity of documents or the identification of the ultimate beneficial owner.

- There is knowledge of previous suspicion of money laundering or terrorism financing concerning the person.
- The customer representative's appearance or behavior may suggest potential involvement in illegal activities.
- The customer is a cash-intensive business operator handling large amounts of cash.
- The customer or the associated company has nominee shareholders or bearer shares (the use of any nominee shareholders or nominee arrangements should be strictly avoided as it represents a risk that cannot generally be mitigated).
- The customer has a limited or inconsistent business history and may lack a solid reputation or compliance record.
- The customer's ownership structure is complex, opaque, or involves nominee shareholders, making it difficult to determine the ultimate beneficial owner.
- The customer's residency or domicile is in a high-risk jurisdiction known for weak anti-money laundering (AML) or counter-terrorism financing (CTF) measures.
- The customer or individuals associated with them hold citizenship in a high-risk country identified by reputable international bodies.
- The customer or individuals associated with them hold prominent public positions, such as high-ranking government officials or politically exposed persons (PEPs).
- The customer has a history of involvement in suspicious or fraudulent activities, including prior instances of money laundering or terrorism financing.
- The customer's source of funds and wealth is unclear, unverifiable, or suspected to be illicit.
- The customer has inadequate or ineffective internal controls, policies, and procedures to prevent money laundering, fraud, or other financial crimes.
- The customer has been subject to regulatory investigations, enforcement actions, or significant fines for compliance violations.
- The customer has connections to known criminal or terrorist organizations, or their activities raise suspicions of involvement in illicit enterprises.
- The customer has a negative reputation or adverse feedback from industry peers, regulatory authorities, or financial institutions.

3. Customer Due Diligence (DD)

3.1 B2B relationships

Torrero Platform N.V. will also conduct due diligence exercises before entering any business relationships with third parties. These exercises will be carried out by senior management together with the legal department and the MLRO. Customer due diligence (DD) will seek to identify what risks would emerge should Torrero Platform N.V. engage in business with the third party. In carrying out this assessment, it will be determined whether the source, nature, and volume of business to be introduced via the third party can be established. Torrero Platform N.V. will also give a lot of weight to the fact that a supplier is already an approved supplier. It is also considered positive if a supplier that is presently not approved seeks approval at the point in time when contracting with Torrero Platform N.V. The assessment will also seek to establish whether the third party has business dealings with other third parties which are known not to be reputable, or if the third party conducts its business in or from a non-reputable jurisdiction. In this regard, Torrero Platform N.V. will ask the third party to provide it with original/certified copies of all the necessary documentation, including, company incorporation certificate, memorandum and articles of association, certificate of good standing, annual financial statements, identification of officers of the company as well as a shareholders list, and a bank reference letter, confirming that the company's affairs are dealt with in a good manner. Once it has been determined that the third party conducts business in a manner which will not jeopardize Torrero Platform N.V. position, then the parties will agree on the terms of the business relationship and sign the relevant agreements and documentation. As part of the DD, Torrero Platform N.V. will conduct ongoing monitoring to ensure that the third party still conducts its business in a diligent manner, based on their own experience of the manner in which the services are provided. Furthermore, Torrero Platform N.V. also reserves the right to include a Right to Audit clause in the agreement it signs with the third party if this is deemed necessary.

Any anti-money laundering review conducted will be separately noted in the third party's file. In any case, Torrero Platform N.V. will always reserve its right to terminate its business relationship with any

third party should it feel that in conducting business with the third party, it is putting its compliance with its anti-money laundering and funding of terrorism obligations at risk. Notification to the relevant authority will be given as per the agreement and as per the requirements of the same authority.

Due diligence measures for low-risk (tier 1) customers:

- Verification of the customer's identity through reliable and independent sources, such as government-issued identification documents.
- Confirmation of the customer's legal existence and business registration, including obtaining necessary documentation and conducting appropriate checks.
- Assessment of the customer's reputation and track record, including reviewing their business history and conducting reference checks if necessary.
- Assessment of the customer's ownership structure and identification of beneficial owners, ensuring transparency and compliance with relevant regulations.
- Screening the customer against relevant sanctions lists, watchlists, or politically exposed person (PEP) databases, to ensure they are not associated with high-risk individuals or entities.
- Analysis of the nature of the customer's business activities, including an understanding of their industry, business model, and transaction patterns.
- Ongoing review and periodic updates of customer information to ensure accuracy and relevancy.

Due diligence measures for medium-risk (tier 2) customers:

- Verification of the customer's identity using reliable and independent sources, such as government-issued identification documents.
- Confirmation of the customer's legal existence and business registration, including obtaining necessary documentation and conducting appropriate checks.
- Assessment of the customer's reputation and track record, including reviewing their business history and conducting reference checks if necessary.
- Evaluation of the customer's source of funds and wealth to ensure they are legitimate and traceable, without any indications of illicit activities.
- Assessment of the customer's ownership structure and identification of beneficial owners, ensuring transparency and compliance with relevant regulations.
- Review of the customer's financial statements, including assessing their financial stability and reliability.
- Screening the customer against relevant sanctions lists, watchlists, or politically exposed person (PEP) databases, to identify any potential higher-risk associations.
- Analysis of the nature of the customer's business activities, including understanding their industry, business model, and transaction patterns.
- Ongoing monitoring and periodic reviews of customer information to ensure accuracy and relevancy.
- Enhanced scrutiny of the customer's relationships with high-risk countries, politically exposed persons (PEPs), or other potentially higher-risk entities.

Due diligence measures for high-risk (tier 3) customers:

- In-depth assessment of the customer's legal existence, including scrutinizing business registration documents and conducting extensive background checks.
- Rigorous investigation into the customer's reputation, including examining their business history, industry standing, and conducting thorough reference checks.
- Detailed examination of the customer's ownership structure and beneficial ownership, utilizing enhanced due diligence techniques to uncover complex ownership arrangements or nominee arrangements.
- Extensive screening of the customer against global sanctions lists, watchlists, and politically exposed person (PEP) databases, as well as conducting heightened scrutiny of associated individuals and entities.
- Intensive review of the customer's financial statements, conducting forensic analysis if necessary, to assess financial stability, consistency, and the absence of suspicious

transactions.

- Engagement of specialized third-party services, such as forensic auditors or investigators, if deemed necessary to conduct deeper investigations or due diligence on high-risk clients.
- Collaboration and information sharing with relevant regulatory authorities and law enforcement agencies, as appropriate, to ensure the highest level of risk mitigation and compliance.

Criteria for imposing restrictions on business relationships with clients:

- Presence on sanctions or watchlists: If a client or associated individuals/entities are listed on national or international sanctions lists or watchlists, it may result in restrictions or prohibitions on business relationships.
- Politically Exposed Persons (PEPs): If a client or associated individuals hold prominent public positions, such as high-ranking government officials or their immediate family members, enhanced due diligence measures may be required, and restrictions may be imposed based on the risk assessment.
- High-risk jurisdictions: If the client or their activities are associated with countries or regions identified as high-risk for money laundering or terrorism financing, additional due diligence measures may be necessary, and restrictions may be imposed depending on the level of risk.
- Criminal activities: If there are reasonable grounds to suspect that a client or associated individuals/entities are involved in criminal activities, including money laundering, fraud, or other illicit practices, restrictions may be imposed to prevent further engagement.
- Lack of necessary documentation or information: If a client fails to provide the required identification documents or other necessary information, or if the information provided is insufficient or unreliable, restrictions may be imposed until satisfactory documentation or information is obtained.
- Failure to pass due diligence assessments: If a client or associated individuals/entities fail to pass the due diligence assessments conducted by the business, which may include identity verification, source of funds verification, or beneficial ownership identification, restrictions may be imposed as a precautionary measure.
- Adverse reputation or negative public information: If there is significant adverse media coverage, negative reputation, or public information about a client or associated individuals/entities that indicates involvement in illicit activities or reputational risks, restrictions may be imposed to protect the business's integrity.
- Material misrepresentation or fraud: If a client or associated individuals/entities are found to have provided false or misleading information, or engaged in fraudulent activities, restrictions may be imposed to safeguard against potential harm or illegal activities.

4. Reporting suspicious activity and transactions

4.1 Appointment of the Money Laundering Reporting Officer (MLRO)

While the detailed description of the responsibilities of the MLRO is laid out in the Human Resources Roles and Responsibilities Policy, the MLRO's main responsibility will be that of considering any internal reports of unusual or suspicious transactions that are raised within the company, and, following up on these reports and filing a STR, when this is deemed necessary. The MLRO, will also act as the main channel through which any communications with the FIU will be conducted. He or she will ensure that Torrero Platform N.V. is effectively implementing the policies and procedures which it has adopted in order to address its anti-money laundering/countering of funding of terrorism obligations. The MLRO will be responsible for monitoring any updates on applicable sanctions lists.. He or she will then update the rest of the staff on any amendments to the sanctions lists and any fundamental changes to the applicable law. Torrero Platform N.V. will ensure that the individual appointed as MLRO enjoys sufficient seniority and command to be able to act independently of its management.

The MLRO will have access to all the necessary information/documentation and company employees to effectively carry out his obligations. Torrero Platform N.V. has also appointed a designate employee who would be able to act as the MLRO during the MLRO's absence.

4.2 Reporting suspicious activity and transactions

Torrero Platform N.V. may develop a suspicion or have reasonable grounds to suspect that activity on

an account is linked to money laundering or funding of terrorism. At that point in time, Torrero Platform N.V. will ensure that all DD requirements are met, regardless of whether any applicable threshold has been met. It will consequently submit a STR as soon as possible.

4.2.1 Internal Reporting Procedures

All staff communicating with the customers, or having access to information about clients' affairs, will receive anti-money laundering training. In this manner, they would be able to identify which customer's action should reasonably lead them to suspect that money laundering or funding of terrorism activity is being attempted or has been carried out.

There may be instances wherein the manager disagrees with the officer, but the officer still feels he has reasonable grounds to suspect wrongdoing. In such circumstances, the employee is to inform the MLRO anyway of his suspicions. The employee may discuss the matter directly with the MLRO and is in no way obliged to inform or involve his manager. On receipt of the internal report from the employee, the MLRO will acknowledge its receipt in writing, referring to the report by its date and unique file number, without including the name of the person(s) suspected. In this manner, the officer's legal obligation to report will be considered to have been fulfilled. The employee will only be allowed to discuss the matter internally with management, or with other employees, if at all deemed necessary, after having obtained approval from the MLRO. Any external discussions are prohibited and will be considered as tipping off. If circumstances arise that make it difficult for the employee to communicate with the player without risking any possibility of tipping off, the employee is to seek advice and follow the MLRO's instructions. This procedure shall constitute Torrero Platform N.V. internal procedure for reporting suspicious activity and transactions.

4.2.2 External Reporting Procedures

As already described in the previous section, the MLRO shall receive and evaluate internal suspicion reports. He will open and maintain a log detailing the progress related to each report, noting down any information which needs to be documented so as to ensure that an adequate track record of the reasons leading to his decision are maintained. Such documentation may also be used to assist the Authorities in any analysis or investigation of the suspected money laundering or funding of terrorism when such details are directly requested from the MLRO. This log shall be held by the MLRO and shall only be accessible to him and will not form part of the customer's file. The MLRO shall gather all the necessary information and pose any questions to any of Torrero Platform N.V. employees as part of his investigation. The employees (whether those having submitted the internal report or otherwise) shall provide the MLRO with relevant information. In doing so, they will not be breaching their obligation of client confidentiality. No copies of either the internal or external reports will be made. The MLRO will keep such records secure. The MLRO shall, where appropriate, inform the originator of the internal report whether a formal disclosure has been made. Following a formal disclosure, the MLRO shall take such actions as required by the Authorities in connection with the disclosure and accordingly follow their instructions.

For clarity's sake, STR reporting will cover:

- Any activity which leads Torrero Platform N.V. to think that a person is linked to money laundering/funding of terrorism or to any proceeds of crime, or that either of the two is being committed, or may be committed, independently of whether any transactions have taken place or otherwise.
- Any instance wherein objective facts will lead Torrero Platform N.V. to have reasonable grounds to suspect that money laundering/funding of terrorism or of proceeds of crime may be taking place.

4.2.3 Stopping/continuing work following a suspicion

Due to the nature of the gaming products and services offered by Torrero Platform N.V., and the nature of the transactions in question, Torrero Platform N.V. will not always be in a position to refrain from carrying out a pending transaction prior to the filing of a STR. This is because should Torrero Platform N.V. refrain from accepting a transaction when it usually does so instantly, the delay in acceptance may trigger the customer into knowing that he is being suspected of fraudulent activity. Any delay may prejudice an analysis or investigation of the suspected transaction. Hence, whenever Torrero Platform N.V. suspects money laundering/funding of terrorism, then Torrero Platform N.V. will still proceed with executing the suspected transaction. However, Torrero Platform N.V. will, submit an STR immediately after the execution of the transaction.

5. Training

It is the policy of Torrero Platform N.V. that all staff who have client contact, or access to information about clients' affairs, shall receive anti-money laundering training to ensure that their knowledge and understanding is at an appropriate level. Training will furthermore be provided at least once a year so as to maintain awareness and ensure that the company's legal obligations are met. Any training given will take into consideration the practicality of assigning different tasks to staff as per their role, and all information accessible will be on a need-to-know basis. However, training about the whole process will be provided to employees, so as to ensure that each officer has a holistic understanding of the due diligence, KYC, AML and payout procedures, since these are very closely related.

In light of the seriousness of the obligations placed by law and regulations, and the gravity of the possible penalties, the MLRO shall ensure that information about these obligations is available to all members of staff at all times. The MLRO will also ensure that on-going training is provided, that is, as and when the need arises, even based on direct requests made by employees.

The training programs will include testing to ensure that each individual has achieved the appropriate level of knowledge and understanding. Testing may be conducted in various ways, whether through formal testing, assessment via discussion of case studies, or other means. Special consideration will be given to the training needs of senior management, and of the compliance team, whose knowledge and understanding must be most thorough.

The Human Resources (HR) Department will:

- ✓ inform every member of staff of the training programs that they are required to undertake, and the timetable for completion;
- ✓ check that every member of staff has completed the training programs assigned to them, issuing reminders to any who have not completed the programs as per the applicable timetable;
- ✓ keep records of training completed, including the results of tests or other evaluations demonstrating that each individual has achieved an appropriate level of competence;
- ✓ update employee personal files with details of training undertaken and results obtained where applicable;
- ✓ refer to senior management any cases where members of staff fail to respond or whose results are unsatisfactory, to issue reprimands or provide additional training as per the individual case.

The MLRO will be provided with full access to all records held by the HR Department.

On completion of a training cycle, the HR Department will ensure the continuity of ongoing training and also obtain updates from the MLRO in respect of changes happening in the field, so that the HR may ensure that up-to-date training is organised and provided to all members of staff.

Line managers will also provide feedback to the HR Department in respect of:

- ✓ the effectiveness of the programs completed; and
- ✓ make suggestions as to different methods of delivery.

Line managers will supplement the training provided to support staff by giving guidance on a day-to-day basis on:

- ✓ the type of client instructions and transactions that count as 'significant' and so should be brought to their attention
- ✓ identifying client instructions and transactions which, although not of a nature normally counting as 'significant', are in some way unusual or anomalous and should be considered regarding possible suspicion of money laundering or funding of terrorism.

The MLRO will determine the training needs for his/her own role and ensure that he/she undergoes Continued Professional Education (CPE) as required to fulfil his/her legal obligations.

The aim of all training provided is to ensure that staff can identify any attempted or actual money laundering or funding of terrorism activity exercised by players when using Torrero Platform N.V. services.

6. Keeping records of client due diligence information

When information is being collected for DD purposes, the responsible service staff will:

- ✓ keep records in the client file.
- ✓ record instances where information requested has not been forthcoming, or explanations provided have not been satisfactory.
- ✓ ensure that all records are kept in a consistent manner so that they are accessible by and comprehensible to other authorised members of staff, including the MLRO.

Transaction and customer records from the date of transaction and end of business relationship respectively, are kept as long as Torrero Platform N.V. has a valid legal reason to keep such records. Such reasons are limited only to legal obligations which Torrero Platform N.V. needs to abide by, such as, anti-money laundering obligations, taxation regulations etc. The records are consequently archived.

Should Torrero Platform N.V. determine that a player's record needs to be retained for a prolonged period of time due to the fact that a report has been filed with regards to that player, all relevant records will be retained on the live system and not archived. This is done so as to ensure that Torrero Platform N.V. complies with its anti-money laundering obligations. Once the enquiry / investigation has been completed and the MLRO has been accordingly informed, then the records will be treated similar to all other information and the same archiving policy will then apply.

7. Monitoring and management of compliance

Compliance with this policy shall be constantly tested and ensured. The Board of Directors reserves the right to engage external auditors to examine whether the company is complying with the measures laid out in this procedure. The findings of such audits and any appropriate recommendations for action will be reported to the Board of Directors. The latter will then request for feedback from management.

in respect of the suggestions made by the auditors. Based on the recommendations as well as management's feedback, the directors will take a decision of what processes / procedures to amend or introduce. A timeline for implementation will also be discussed and decided upon. Feedback on the implementation of any changes is to be reported back to the directors since they are ultimately responsible for the company's operations.

The MLRO will obviously be involved, and his input will be deemed paramount in respect of this process. He will be tasked to monitor aspects of the company's DD and anti-money laundering policies and procedures. Any deficiency in these procedures or the compliance thereto, which requires urgent rectification will be dealt with immediately by the MLRO, who will report such incidents to the Board of Directors as appropriate. He will also request the Board to provide him with any needed support.

The MLRO will audit the procedure directly, at least annually. The MLRO will also report his findings to the Board of Directors. This report will include:

- ✓ a summary of any changes in the regulatory environment(s) in which Torrero Platform N.V.

operates.

- ✓ a summary of AML activities within the company, including the number of internal suspicion reports received by the MLRO and the number of disclosures made to the Authorities.
- ✓ details of any compliance deficiencies on which action has already been taken, together with reports of the outcomes.
- ✓ details of any compliance deficiencies on which action needs to be taken, together with recommended actions including suggested timeframe and management support required.
- ✓ an outline of plans for the continuous development of involved staff, including periodic training and awareness raising activities for all relevant staff.

Where management action is indicated, the Board of Directors will request management to provide their feedback and timeline of when necessary, action will be taken.

This procedure will be reviewed and updated at least every six months. However, this may take place more frequently, if changes in legislation or guidelines are introduced at any point in time, or if deemed necessary.