

AML & KYC Policy

GENERAL

Policy Statement

It is the policy of puntpal that all members of staff shall actively participate in preventing the services of puntpal 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 puntpal's 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 puntpal 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 puntpal 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 puntpal's 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.

Definition

puntpal believes that prior to implementing its Fraud Management Procedure, 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, so as 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 organizations 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.

THE RISK BASED APPROACH

Definition

As per the applicable laws, puntpal 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 materializing. The approach, allows for flexibility and significant discretion to be exercised by puntpal. This in itself entails significant responsibility. It is up to puntpal 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 puntpal will adopt so as 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.

Risk Assessment

Risk Management entails:

recognition of existence of risk

undertaking of a risk assessment, and

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 so as to ensure that the risks which puntpal has identified and which it will face as part of its operations will not materialize. puntpal's organizational risk assessment which is to be approved by the Board of Directors takes the following factors into consideration:

Product/Service/Transaction Risk

Some gaming products/services/transactions are more vulnerable to criminal exploitation than others. These include, for instance, gaming products or services that allow the customer to influence the outcome of a game, be it one player alone or in collusion with others.

Interface Risk

This refers to the channel through which puntpal establishes a business relationship and/or through which transactions are carried out. Non face-to-face interactions, such as in respect of puntpal's 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. puntpal 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 puntpal 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 puntpal was justified in considering that the customer is actually the persons he alleges to be.

Geographical Risk

This is the risk posed to puntpal 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 fraud management procedure is primarily that attributable to the customers and the source of funds of the said customers. The nationality, residence and place of birth of a customer 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.

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, puntpal 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 of the relevant indicators will be taken into consideration. These together, determine the player's risk profile contributing to the totality of a player's risk profile.

Customer Risk

This relates to the type of customer being provided with the service. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. In identifying the level of risk inherent in a relationship, puntpal will be assessing what would be the likelihood that a customer would be able to launder proceeds of crime through puntpal's service. A high earning customer who spends a fourth of his monthly wage in wagering is not likely to constitute a high risk, even if the amount being wagered is large. On the other hand, a minimum wage earner who spends his only wage on wagering will more likely constitute a high risk. Furthermore, the individual 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.

CUSTOMER DUE DILIGENCE (CDD)

Procedure

The Fraud Management Procedure will now focus on the getting-to-know the customers procedure and identifying the risks related to their transactions and the origination of their funds, both from where the funds were obtained as well as the source of the funds from where the customer has remitted the funds.

As described above, a risk assessment can never be a one-size-fits all exercise. puntpal will in this respect carry out a risk assessment upon entering into a business relationship with, or carrying out an occasional transaction for a customer. For the purposes of clarity, puntpal will not be accepting corporate players only individual players. The mentioned risk assessment will allow puntpal to develop a risk profile concerning the customer and categorize the risk as low, medium or high, thereby allowing it to identify the controls which need to be adopted. The player's risk profile will not be completed upon registration. The registration part of the process will only signify the start of the collection of information, and as such the risk profile will be increased and refined with the development of the relationship with the player. Having said that, should there be a change in the business relationship entertained with the customer, which therefore also entails a change in the risk identified, the measures adopted to control the risk shall be adapted accordingly. Furthermore, ongoing monitoring, as explained in more detail below, will ensure that any change in risk is spotted as soon as possible. The level of monitoring will be commensurate to the risk posed by the particular customer, but systems will be put in place so as to detect developing risky situations.

To start off puntpal adopts CDD measures so as to determine, who its customers are. All details collected at registration stage are used to build the customer profile. Further customer profiling is done, based on the customer's activity and also on the particular behavioral aspects. This profiling aspect will assist in determining the risk attached to the particular player and thus also facilitate in the identification of future unusual behavior. CDD is divided into the below three parts:

Identification and Verification of the Customer

Identification consists in the collection of the player's personal details. This information is collected during the registration process. The personal

information to be collected is to start off the Know Your Client (KYC) procedure, which includes the collection of the following personal details:

Name and surname

Permanent residential address

Date of birth, as the player has to be over eighteen years of age (or any other age as applicable in the player's particular jurisdiction)

Valid email address

Place of birth

Nationality, and

Identity reference number where applicable.

Once the above information is provided, puntpal will first ascertain whether the individual in question is a Politically Exposed Person (PEP), a family member of the PEP, or a close business associate of the PEP. A reliable electronic database, such as [opensanctions.org](https://www.opensanctions.org) and [complyadvantage.com](https://www.complyadvantage.com) will be integrated and made use of in this regard. If it is determined that an individual is a PEP or in any way related to a PEP, then the individual will be deemed himself / herself a PEP and will not be allowed to register as a player with puntpal, as the latter has a strict policy of not accepting PEPs as players. This therefore means that determination as to whether an individual is a PEP (as per above definition) will take place at registration stage.

The account will be formally opened once the player's e-mail has been verified. In any situation where the player is immediately identified as being high risk, puntpal may immediately ask for additional personal details and for verification of the same details provided. In any case, puntpal will ensure that it is at all times able to determine that the customer is who he claims to be and that the measures adopted are effective enough to counteract the risk of identity fraud and impersonation.

Verification consists in confirming the personal details collected for identification purposes through the use of independent data, information and documentation obtained from reliable sources. If inconsistencies in the personal information provided by the customer are identified, puntpal will consider whether to adopt additional identification and verification measures.

This will take place by either of two ways:

Documentary sources,

As a rule, this method of verification will be carried out by making reference to Government- issued documents containing photographic image together with the player's identity (e.g. passport, identity card, driving licence etc). If the player's residential address cannot be verified by using any one of the just mentioned documents, puntpal will ask for alternative reliable documents such as a recent utility bill, bank account statements, correspondence from Government or public entities etc, so as to be able to verify the address. The documents requested will be received by electronic mail and if deemed necessary notarized documents may be requested for.

puntpal will ensure that all documents received are clear, legible, of good quality, and are authentic or reflect authentic ones. Some documents, such as passports may be easier to verify as these can be checked against other sources. In other cases, such as with regards to utility bills, the verification process may be less easy. puntpal will carry out additional checks by using specific software programs / applications; that will be integrated as a solution to assist users in conducting their work.

In respect of the validity of the information provided, puntpal will also consider other data that is collected from the player such as geo-location, IP address data etc. that should under normal circumstances corroborate the data contained in the documents provided by the player. There will be exceptions, where the IP address will not tally with the country / location. Such instances would need to be checked on a case by case basis and verification / clarification will be obtained directly from the player.

Electronic means

These include sources like E-ID or Bank-ID and electronic commercial databases. puntpal is well aware that the reliability of these databases may not always be the best. In this regard it will consider what source of information is feeding into the database and whether such data is generally known to be maintained up to date. When making use of the mentioned electronic databases, puntpal will also make use of other documentary evidence for better confirmation / reliability. This is because a positive result on the electronic database will only mean that there is an individual whose personal details correspond to those provided by the client, but not that the client is that individual. On the other hand, when using electronic sources like E-ID and Bank-ID, which can be accessed only through the use of credentials held by a specific individual, no

additional verification means will be requested, as these sources are deemed to provide a sufficiently strong link.

Obtaining information on the purpose and intended nature of the business relationship

The objective behind the opening of a gaming account is quite self-evident and hence no clarifications as to why an account opening request has been made will be sought. However, there may be an ulterior motive on the basis of which the account was opened possibly even being, for money laundering or funding of terrorism. If puntpal has any suspicion that such an ulterior motive subsists, the nit will conduct further investigation and request for additional data and documentations to either justify its suspicions or else to confirm that indeed there are no justifiable indications of an illegal motive.

There is no specific timeframe or period when these additional checks will be conducted, as these will be simply carried out when the suspicion arises. Hence the investigation may need to be conducted upon registration, whereas in other instances it will not need to be carried out until the specific mandatory AML thresholds are reached.

In the event that any checks are to be carried out prior to the mandatory period, puntpal will first collect sufficient information, and where it is necessary, documentation to establish the player's source of wealth. Identifying the player's source of wealth consists of determining the activities which generate the player's net worth, which will then lead puntpal to determine whether this amount of wealth justifies his projected and actual level of account activity. puntpal will at this stage also profile the player within the player risk matrix (as per the table in the next section). Where the risk determined following the checks is medium or low, puntpal will accept a declaration from the customer with details, such as nature of employment/business, and a declaration regarding annual salary. Searches on professional networks and social media will also be used for verification purposes. If the risk is high or puntpal has doubts as to the veracity of the information collected, the player will be requested to provide further independent and reliable documentation which evidences the alleged source of wealth. So, for instance the individual may be asked to mail out a copy of his pay slip or providing such other documented evidence to confirm his declaration.

Ongoing Monitoring

This ultimately entails the monitoring of clients' transactions, personal details and changes in their circumstances or wagering preferences, so as

to ensure that they are consistent with the anticipated activity, and if not, to identify why the changes have occurred. The aim is that subjectively unusual large transactions, changes in gaming patterns and other 'out-of-the-ordinary' activities will be identified and analyzed. In this respect, it is important for puntpal to ensure that the players' information is maintained up-to-date. It will encourage and even oblige players via the terms & conditions to inform puntpal of any changes, and possibly provide documentation to confirm the same. Through the monitoring process, the risk level will be reviewed and an analysis of whether the previously established risk rating should be amended or not will be carried out. Any inconsistencies in information would need to be justified and puntpal reserves the right to request for further corroborating evidence.

Adequate ongoing monitoring also entails carefully examining the player's transactions and playing patterns so as to ensure that these are in line with puntpal's knowledge of the player, his gaming activity and risk profile. If the two do not coincide, then puntpal will similarly question the situation. Whenever puntpal asks for further information, it will always take note of its findings so as to evidence its compliance. Should any identified inconsistency persist without it being successfully addressed, puntpal will analyze whether any report is to be submitted to the relevant authorities and also take a decision whether it deems it necessary to suspend the player's account.

The below screenshots provide an example how puntpal will be able to keep track of which due diligence documents have been requested, received, and any other related notes:

Lastly, with regards to PEPs, a scenario may arise wherein a player may not have been considered to be a PEP at registration stage, but becomes one during the course of the business relationship. If, when conducting on-going monitoring puntpal becomes aware of such a change, puntpal will terminate its business relationship as it has a strict policy of not accepting PEPs as players. Should it be the case that for some reason or another, the individual had not been identified to be PEP even if s/he was a PEP at registration stage, but is consequently identified to be such, puntpal will void any winnings obtained by the individual, and will then transfer deposited funds, to the original source from where the funds originated. It will consequently close the player's account, as per the procedure laid out in section 3.3 below.

TIMING AND APPLICATION OF CDD MEASURES

As described further above the player's account will be successfully opened once the player registers providing the requested basic personal information, and subsequently verifying his email address via the e-mail activation link. The system is set to prevent minors from registering by rejecting any date of birth inserted which would signify that the player is under eighteen years of age (or any other age as per specific legislation – such as Latvia – 21 years of age.)

Any player details' verification (with the exception of PEP confirmations) may occur at any point in time at puntpal's discretion. However at least, it must definitely be carried out when

the amount deposited by the players reaches the cumulative value of € 2,000. It makes no difference whether such deposits have been carried out via a single operation or several operations which appear to be linked or otherwise. puntpal will hence put in place a system which calculates on a daily basis, whether, the player has reached the deposit limit of € 2,000 on his account. Another important factor that the system will include is, the identification of possible multiple accounts, which accounts would have been specifically created to either defraud the company through bonuses abuse or specifically to never reach the required deposit limit of €2,000, and hence ensuring that the account remains unverified.

Up until the time that this threshold is reached, puntpal will conduct ongoing monitoring as per point C of section 3.1 above, so as to ensure that player information is still correct. Furthermore, if puntpal notices at any point in time any inconsistencies between the information provided by the player and any other information it acquires, puntpal will question the discrepancies and take any remedial action it deems necessary. In addition, should suspect money laundering or funding of terrorism be suspected, it will follow the procedure laid out in section 4 below.

Once the mentioned threshold is reached, the player's risk profile will be confirmed, upon the basis of the risk assessment carried out as per section 2.2 above. The latter shall take place prior to the lapse of thirty days from when the € 2,000 threshold is reached. The risk assessment will determine whether the risk posed by the individual is low, medium or high. The measures adopt to control the risk in question vary, as per the table laid out hereunder:

Risk Identified Measures Adopted

Low

Verification of Personal Details

On-Going Monitoring is carried out to ensure relationship remains Low Risk and threshold is not exceeded again

Any suspected cases of money laundering or funding of terrorism are to be reported

Medium

Additional personal details as deemed necessary by puntpal are collected

Verification of Personal Details takes place by using documents containing photographs of the individual

Source of Wealth information is collected

Ongoing monitoring is carried out so as to be able to detect unusual activities, and also to keep information and profile updated

Any suspected cases of money laundering or funding of terrorism are to be reported

High

Additional personal details as deemed necessary by puntpal are collected

Verification of Personal Details takes place by using documents containing photographs of the individual

Source of Wealth information and documentation is collected

Ongoing monitoring is carried out even more thoroughly and at more frequent intervals than that carried out for medium risk, so as to be able to detect unusual activities, and also to keep information and profile updated

Source of Funds may need to be determined for specific transactions

puntpal will allow players to continue using their gaming account while it is still obtaining necessary information and/or documentation from the player concerned. However, up until the time when puntpal actually obtains the mentioned information and/or

documentation, and verifies the player's identification, it will not allow the player to make any withdrawals from his account, independently of the amount involved. Furthermore, if thirty days have lapsed from when the €

2,000 threshold has been met, and the player has not provided the requested information and/or documentation puntpal will terminate the business relationship with the player, following the procedure laid out in the next section.

TERMINATION OF THE BUSINESS RELATIONSHIP

puntpal will terminate its business relationship with a player if he fails to provide the requested information and/or documentation, which puntpal has repeatedly requested of him. puntpal will void any winnings and will then transfer deposited funds to the original source from where the funds originated. All approval for such action must be taken by senior management and only once it has ascertained that there is no restriction on the transfer of the funds. If puntpal finds it impossible to remit the funds back to the player through the same channels, it will, as a measure of last resort, remit the funds to a single account held with a credit or financial institution in a reputable jurisdiction in the player's name. If no such account is made available then the funds will continue to be held in the players' name. The funds will continue to be held on account until the player provides adequate details for the transfer. If this never materializes then after the lapse of 30 months any funds remaining on account will be remitted to the Malta Gaming Authority (CURACAO GAMING AUTHORITY). Whenever remitting such funds, puntpal will indicate in the instructions accompanying the funds that these are being remitted due to inability to complete CDD. puntpal will also consider whether there are grounds for filing a Suspicious Transaction Report (STR), as per the procedure laid out hereunder.

B2B RELATIONSHIPS

puntpal will also conduct due diligence exercises before entering into any business relationships with third parties. These exercises will be carried out by senior management together with the legal department and the MLRO. Just like CDD, business due diligence (BDD) will seek to identify what risks would emerge should puntpal 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. puntpal will also give a lot of weight to the fact that a

supplier is already an approved supplier as per CURACAO GAMING AUTHORITY requirements. It is also considered positive if a supplier that is presently not approved seeks approval at the point in time when contracting with puntpal. 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, puntpal 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 puntpal's position, then the parties will agree on the terms of the business relationship and sign the relevant agreements and documentation. As part of the BDD, puntpal 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, puntpal 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, puntpal 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 CURACAO GAMING AUTHORITY will be given as per the agreement and as per the requirements of the same authority.

RELIANCE AND AGENTS

puntpal may decide to rely on the information and documentation collected at customer on-boarding stage by a third party, and/or engage an agent. In either of the cases, puntpal will ensure that the third party is established in an EU Member State or a reputable jurisdiction which adopts the same anti-money laundering or countering of funding of terrorism measures as laid out in the applicable Maltese laws, or measures which are equivalent thereto. In determining the latter, puntpal will rely on reputable sources such as the Financial Action Task Force on Money laundering evaluation reports, IMF Country Reports, etc.

If puntpal decides to rely on information provided by a third party, it may still request the player to provide it with any verification documents. In such circumstances, puntpal will still conduct the customer-based risk assessment itself, determine the customer's risk rating and conduct on-going monitoring. The relationship between puntpal and the third party will be laid out in an agreement, and one of the conditions will be that of the third party providing puntpal with documents concerning players, immediately upon request. puntpal will also include a Right to Audit clause in the agreement and will indeed periodically test this arrangement, to ensure that the necessary player personal details and documentation is being collected as per the agreed specifications.

A copy of this procedure will also be provided to the third party so as to ensure that the CDD requirements and applicable thresholds are adequately communicated, and thus the third party will never have the excuse that they were not aware of what the applicable company requirements are. puntpal may, whenever allowed by law, opt to use the services of agents in order to on-board or service customers. puntpal may request the agent to carry out the necessary anti-money laundering/countering of funding of terrorism controls and adoption of measures when on-boarding or servicing one of puntpal's customers. In any case however, puntpal will ensure that any application of CDD measures is carried out diligently and as required by the applicable laws. puntpal is well aware that in exercising reliance or making use of agents, it remains ultimately responsible for ensuring it is adhering to its anti-money laundering/countering of funding of terrorism obligations.

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 also filing a STR with the Financial Intelligence Analysis Unit (FIAU), when this is deemed necessary. The MLRO, will also act as the main channel through which any communications with the FIAU will be conducted. He will ensure that puntpal 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 sanctions lists such as that of the Financial Action Task Force (FATF) and the Office of Foreign Assets Control

(OFAC). He will then update the rest of the staff on any amendments to the sanctions lists and any fundamental changes to the applicable law. puntpal 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. puntpal has also appointed a designate employee who would be able to act as the MLRO during the MLRO's absence. The MLRO's as well as the designate employee's appointments will be made known to the CURACAO GAMING AUTHORITY, so that the CURACAO GAMING AUTHORITY, as well as the FIAU, may address queries and requests directly to them, whenever the need arises. Thus, such individuals will act as a contact point between puntpal and the relevant authorities in matters related to anti-money laundering/countering of funding of terrorism.

REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS

puntpal 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, puntpal will ensure that all CDD requirements are met, regardless of whether any applicable threshold has been met. It will consequently submit a STR as soon as possible.

INTERNAL REPORTING PROCEDURES

As laid out in further detail in section 6 below, all staff communicating with the players, or having access to information about clients' affairs, will receive anti-money laundering training. In this manner, they would be able to identify which player's action should reasonably lead them to suspect that money laundering or funding of terrorism activity is being attempted or has been carried out. For instance, they would be expected to realize that if a player attempts to register more than one account with puntpal, or if he deposits considerable amounts during a single session by means of multiple pre-paid cards, then such actions should constitute indicators or red flags which should lead them to question the player's behavior. At that point, the employee may subtly seek explanations from the player, without disclosing his suspicion to the player. This disclosure is forbidden whether directly or indirectly, and hence all members of staff must be astute in this respect. If the officer does not manage to obtain any convincing

information, and after full consideration the officer is still suspicious of foul play, then at that point he shall inform his immediate superior. Obviously enough, prior to reporting to his superior, the employee will have to be satisfied that there is a clear indication of intent to circumvent the safeguards, and that use of the financial system for criminal purposes is present.

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 puntpal's internal procedure for reporting suspicious activity and transactions.

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 player's file. The MLRO shall gather all the necessary information and pose any questions to any of puntpal's 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. Once the MLRO decides that there are

reasonable grounds which warrant the submission of a STR via the Authority's online submission system, he shall make this formal disclosure to the FIAU on behalf of puntpal. 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 or not 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.

What should give rise to a suspicious activity? For clarity's sake, STR reporting will cover:

Any activity which leads puntpal 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 puntpal to have reasonable grounds to suspect that money laundering/funding of terrorism or of proceeds of crime may be taking place.

puntpal shall be obliged to submit an STR with the FIAU with regards to activity carried out on the basis of its Curacao Gaming License, and accordingly notify the CURACAO GAMING AUTHORITY, when deemed necessary and as per instructions given by the FIAU.

Stopping/continuing work following a suspicion

Due to the nature of the gaming products and services offered by puntpal, and the nature of the transactions in question, puntpal 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 puntpal refrain from accepting a transaction when it usually does so instantly, the delay in acceptance may trigger the player into knowing that he is being suspected of fraudulent activity.

Any delay may prejudice an analysis or investigation of the suspected transaction. Hence, whenever puntpal suspects money laundering/funding of terrorism, then puntpal will still proceed with executing the suspected transaction. However, puntpal will, submit an STR to the FIAU immediately after the execution of the transaction.

PROHIBITIO OF DISCLOSURE

puntpal will not disclose any details or information in connection with a STR or a request for information made by the FIAU. This prohibition of disclosure applies with regards to both the suspected player and any other third party, and this independently of any other regulatory or contractual obligation that puntpal may be subjected to. puntpal will only make the necessary disclosures to the CURACAO GAMING AUTHORITY, as prescribed by the applicable law. It will also be extremely careful when dealing with a player that is the subject of a STR or FIAU enquiry. As explained above, this is so as not to prejudice an analysis or investigation. The exceptional cases wherein the prohibition of disclosure does not apply are mentioned under Regulation 16(2) of the Prevention of Money Laundering and Funding of Terrorism Regulations, 2017, and will apply as follows:

- Disclosures to the supervisory Authority, in this case the CURACAO GAMING AUTHORITY;

- Disclosures between subject persons in the same group;

- Disclosures between a subject person undertaking a 'relevant activity' and another person undertaking similar activities and where similar requirements are imposed by the jurisdiction. The persons being within the same legal person or within a larger structure to which they belong, which have common, ownership, management;

- Sharing of information based on the same transaction, where the subject persons and the related activity are subject to the same legal obligations and the persons are of the same professional category and hence have similar obligations in respect of professional secrecy and data protection;

- Disclosures by a subject person in the course of proceedings initiated in respect of delays in carrying out transactions, where the subject person was actually following instructions as per FIAU;

- Disclosure by a subject person to a supervisory authority as per the request made by the supervisory authority, in this respect, the CURACAO GAMING AUTHORITY.

puntpal will also consider carefully any of the measures which it decides to adopt vis-a- vis the suspected player, consequent to the submission of a STR. So as not to jeopardize any investigation, prior to undertaking any such action, puntpal will seek guidance from the FIAU's analysts. puntpal will, as much as possible, consider such actions as a measure of last resort, and not unnecessarily burden the FIAU with every small suspicion. In cases of minor suspicions not warranting reporting, it will instead

increase on- going monitoring and only submit STRs to the FIAU once a suspicion persists or the indicators increase. puntpal will ensure proper documentation of such internal decision-making.

PAYOUT MANAGEMENT PROCEDURE

Whenever a player makes a withdrawal request, regardless of the payment method used, puntpal will, prior to acceding to such a request, ensure that the institution to which the funds are to be remitted is situated in a reputable jurisdiction and has equivalent anti- money laundering/ counterfeit terrorism requirements as are applicable to puntpal. Obviously enough this also ties in to the institutions from where player deposits are accepted. As a general rule, withdrawals will only be processed to the same source from where the funds originated. This measure will limit the risk of successful money laundering or funding of terrorism withdrawals.

Furthermore, no cash deposits or withdrawals will be affected. Withdrawal requests shall be carried out as per the following procedure:

Withdrawal requests will be processed immediately upon request.

No cash withdrawals can be processed under any circumstances. Cash transactions are specifically prohibited and in fact there are no methods that players may apply to process any fund transfers in cash.

The gameplay will be checked as well as all financial transactions.

puntpal will also consider whether individuals are playing fairly, or whether the gaming system has in any way been manipulated, or whether the system is, alternatively, malfunctioning, and the player was in any way taking advantage of any bug without, accordingly informing puntpal, as per the Terms & Conditions' requirements.

Reference will also be made as to whether CDD verification has been conducted. If it has not yet been carried out since the deposit requirement was not reached, a management decision is taken as to whether it is deemed necessary to conduct CDD verification at this stage prior to completing the withdrawal process.

The risk assessment is also conducted / checked to ensure that the player's risk vis-a- vis his activity with puntpal is determined.

Applicable CDD requirements will be as per section 3.2 above.

If the player does not provide the necessary documents for verification to take place, when requested, or if it becomes clear that verification cannot take place because the individual has acted fraudulently, withdrawals will not be processed. Once it becomes clear to puntpal that the individual was attempting to act fraudulently, it will block the player's account, void all winnings and simply return the deposit to the account from where the funds originated.

In the event that withdrawals cannot be processed to the account from where the funds originated, such as when the player is making use of Mastercard or Pay-safe-card, then puntpal will formally request for player verification documents and also request for details of another payment system that may be confirmed to be in the player's name and hence minimizing the risk of remitting funds to an individual that is different from the person that had originally remitted the deposits. This process is in place to discourage credit card theft and identity theft.

TRAINING

It is the policy of puntpal 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 organized 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 with regard to 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 is capable of identifying any attempted or actual money laundering or funding of terrorism activity exercised by players when using puntpal's services.

KEEPING RECORDS OF CLIENTE DUE DILIGENCE INFORMATION

When information is being collected for CDD 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 authorized 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 puntpal has a valid legal reason to keep such records. Such reasons are limited only to legal obligations which puntpal needs to abide by, such as, anti-money laundering obligations, taxation regulations etc. The records are consequently archived. The players have the possibility of accessing transactions from their profile for a period of 2 months. Following that time lapse, details about the transactions may be requested through customer support on gmbvcuracao@gmail.com.

Should puntpal 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 puntpal 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.

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

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