

AML POLICY

Bullish Entertainment B. V.

DOCUMENT CONTROL

Version No.	Date	Description	Author	Signature
1.0	01/10/2025	Policy approval	MLRO	

1. Policy Statement	5
2. Purpose	5
3. Audience	5
4. Definitions	5
5. Policy Implementation	6
5.1 Business Risk Assessment (BRA)	6
5.2 Customer Risk Assessment (CRA)	7
5.3 Customer Acceptance Policy (CAP)	8
5.4 Customer Due Diligence	9
5.4.1 Level 1 - Simplified Due Diligence (SDD)	9
5.4.2 Level 2 - Customer Due Diligence (CDD)	11
5.4.3 Level 3 - Enhanced Due Diligence (EDD)	13
5.5 Ongoing Monitoring	17
5.6 Reporting of unusual transactions	18
7. Compliance and Consequences of Non-Compliance	19
8. Contact information	19
9. Policy History	19

1. POLICY STATEMENT

The company takes a zero-tolerance approach to money laundering and terrorist financing activities and is committed to implementing and enforcing effective internal controls to counter such activities. The company's policy is to apply at a minimum the standards set out in this Policy.

2. PURPOSE

The purpose of this Policy is to establish policies and procedures on internal controls, risk assessment, risk management and compliance in relation to AML and CTF.

This Policy may be amended from time to time to reflect updates to the laws and regulations on which it is based.

Curacao's core AML framework is governed by Online Gaming Licensing Ordinance (LOK). The AML framework is designed to prevent and combat financial crimes like money laundering and terrorist financing.

3. AUDIENCE

This Policy is applicable to all employees, contractors, affiliates and any other individual working on behalf of the company. The policy outlines the general and minimum standards of internal AML and CFT which should be adhered to by the company's management, employees and any third party working on behalf of the company.

4. DEFINITIONS

For the scope of this Policy, the following terms shall have these meanings, unless the context otherwise requires:

- a) "AML/CTF" means anti-money laundering and countering the financing of terrorism;
- b) "beneficial owner" means: a natural person who ultimately owns or controls a facility holder; the natural person on whose behalf a transaction is being conducted; or a natural person who exercises ultimate effective control over a legal person or legal arrangement. Where no natural person fits squarely into those categories, it is the person who holds the position of senior managing official.
- c) "CDD" means customer due diligence;
- d) "controlling interest" means direct or indirect shareholders acting individually or as a group holding ten percent (10%) or more of the voting rights and shares in an entity;
- e) "identified risk" means corruption, cybercrime, human trafficking, money laundering, or financing of proliferation of weapons of mass destruction, terrorism or financing of terrorism;
- f) "identified risk framework" means the measures or policies designed to minimize or eliminate identified risks;
- g) "occasional transaction" means a one-off transaction or linked transactions, that are carried out by a person otherwise than through a facility in respect of which that person is a facility holder;
- h) "senior management" means an officer or employee of the company with sufficient knowledge and seniority to make decisions affecting the company's risk exposure which need not involve a member of the board of directors and includes a person responsible for compliance or who is authorised to bind the company;
- i) "source of funds" means:
 - the transaction or business from which funds have been generated, and
 - the means by which a customer intends to transfer those funds/assets to a facility;
- j) "source of wealth" refers to the means by which a customer acquires his/her wealth.
- k) a "document" is a record of information kept in any form, including electronic format.

5. POLICY IMPLEMENTATION

The company has established clear responsibilities to ensure that policies, procedures, and controls which deter criminals from using its facilities for money laundering or the financing of terrorism, are implemented and maintained, thus ensuring that they comply with the obligations under the laws and regulations.

As such, the company has implemented standards and principles which include:

- Establishing and maintaining a risk-based approach towards assessing and managing the money laundering and terrorist financing risks for each of its customers;
- Establishing and maintaining risk-based customer due diligence measures, for the identification and verification of its customers, including enhanced due diligence measures and ongoing customer and transaction monitoring;
- Implementing procedures for reporting suspicious activity internally and to relevant law enforcement authorities, as appropriate;
- Maintenance of appropriate records for prescribed periods;
- Training, awareness-raising sessions, and regular screening.

The company's terms and conditions highlight its commitment to compliance with all applicable laws and regulations. No customer will be onboarded unless they have agreed to the terms of use.

The company will take all reasonable measures to safeguard against the possibility of customers depositing funds originating from criminal activity or depositing funds by using a payment facility for which the customer is not authorized to use. It shall implement measures to make sure that it does not allow activities or transactions that should be prohibited, such as any such activities or transactions linked to illicit activity or fraud.

The company adheres to the three lines of defense to ensure that a level of control is being held and that reporting is carried out efficiently without any unnecessary barriers. The lines of defense are being:

- 1) The first line of defense is the customer facing and customer support, carrying out transaction monitoring, customer execution of due diligence and ensuring that all policies are being adhered to.
- 2) The second line of defense is the AML Compliance Officer and compliance team, who are tasked with the compliance monitoring, point of contact to the regulators, reporting of suspicious transactions, and set policies and standards.
- 3) The third line is the audit function.

The governance structure is to promote immediate reporting to the AML Compliance Officer, ensuring that internal controls and compliance management is also being adhered to, and to also ensure that the audit function may provide an annual gap analysis in order to mitigate any potential risks. The structure also ensures that the decisions are taken at the appropriate level.

5.1 BUSINESS RISK ASSESSMENT (BRA)

The BRA is an encompassing view of inherent risks, vulnerabilities and threats to the company, the mitigating factors conducted and the residual risk. The company's policies, internal controls, compliance management and procedural documentation, is influenced by the BRA.

The residual risk, as a result of the BRA determines whether a particular risk falls within the acceptable risk appetite of the company or if such risk will be outrightly refused. For example, the BRA is conducted prior to the launch of any product to identify the inherent risk associated, mitigating factors, and whether the residual risk of such product fits the company's acceptable risk appetite. If the risk does not fall within the

company's acceptable risk appetite such product's risk mitigators will be increased. If such a product's risk still falls within an unacceptable level, the product will be discontinued.

The factors which are included in the BRA are as follows:

- Product / Service
- Transaction
- Geography
- Customer
- Interface

The manifestation of risk of the factors above are assessed in relation to ML and FT. In developing the operational AML/CTF policy and procedures, the company has reviewed its business processes against the criteria set out above to take a 'risk-based approach' to the development of AML/CTF controls. The BRA summarizes the factors into low, medium and high risk.

New or material changes shall warrant a re-evaluation of the BRA; such changes shall also be applicable upon introduction of new products, services, jurisdictions and payment methods. Changes within the regulatory framework shall also be considered as pertinent elements that shall contribute to a review of the risk.

5.2 CUSTOMER RISK ASSESSMENT (CRA)

The company has developed a robust internal scoring from which the level of due diligence is requested from the customer. The risk assessment is a pertinent aspect in assessing factors which are obtained through the customer profile which is to be provided in detail by the customer. By identifying and assessing the money laundering risks, the company can take the best steps to mitigate and monitor those risks.

Risk factors from which the risk is likely to emanate are from and are prevalent in the company's risk assessment are:

1. Jurisdiction risk
2. Customer risk
3. Interface risk
4. Transaction risk
5. Product and service risk
6. Fraud and behavioral patterns

Understanding the risks that may arise from the above factors, the company has taken up the development of sound risk management practices, to help assist the officers involved in the process and tools to manage the risk posed by the threats of money laundering, funding of terrorism or other illicit activity.

The level of due diligence required is dynamic as the risk depends on the actions and behavioral patterns of the customer. The company has a twofold approach to the CRA:

- Risk assessment: The risk assessment is in place to indicate behavioral patterns and pertinent information emanating from the customer.
- Transactional triggers: These triggers are serious instances which give rise to possible ML/FT therefore all transactional triggers require an internal analysis of the action.

The risk score of the customer shall reflect the customer's current position whether at onboarding or ongoing monitoring. The customer is assigned a score which determines if the customer is Low, Medium or High Risk. Risks may be cleared following a policy assessment and/or the customer providing sufficient

information to clarify any alerts generated by the system. The risk assessment can only be re-evaluated by the AML Compliance Officer, with a written rationale to be left on the customer's account.

Any alerts cleared shall be recorded but shall not affect the risk score of the customer. The risk score can be overwritten if an officer has reasonable doubts. For example, if an officer would like to place a low risk customer as a high risk, if reasonable justification is provided, they can do so.

The risk assessment is pertinent in assessing factors obtained through the profile to be provided in detail by the customer. Each criterion of risk will determine a set level of due diligence for which the information required is readily available from a list of due diligence requirements. A justification for the level of due diligence will have to be provided, including any reasoning behind the assigned risk category.

5.3 CUSTOMER ACCEPTANCE POLICY (CAP)

The company currently has a high risk appetite when it comes to customer acceptance but a medium risk business appetite meaning that the residual risk of any service must have sufficient controls in place to mitigate such risk to be within controllable boundaries and for which the company has control over the behavioral pattern and relationship with the customer.

The policies and procedures hereunder are all reflective of such concepts and are therefore in place to further activate the desired result in ensuring proper risk management and mitigation.

Following the risk-based approach, a risk assessment of the ML and FT risk posed by the customer is carried out based on the information provided by the customer and checks conducted. The risk assessment will rate the customer as low, medium or high risk. Due diligence and ongoing monitoring will be carried out in proportion to this risk. If the risk is deemed Medium or High, further information and documentation is required from the customer. If the account is rated High Risk and/or is exhibiting trends or there is suspicion, knowledge or reason to believe it must be reviewed by compliance personnel and brought to the attention of the AML Compliance officer for further investigation.

The company shall also ensure that in the event a customer is generating funds derived from a non-acceptable business which has been deemed as illegal or immoral, such customer shall be subject to an internal investigation as accounts are to be blocked due to the pretense of a false declaration.

5.4 CUSTOMER DUE DILIGENCE

This section describes the criteria for accepting new customers based on their risk categorisation. Following a risk-based approach for every customer, it will be determined what level of due diligence is to be applied concerning identification, business relationship and transaction level.

Where the level of risk is above the level the Company is willing to accept, appropriate steps must be taken to mitigate the risk. If the risk cannot be mitigated to an acceptable level, the relationship must be terminated.

Upon registration, the customer, shall provide the following identification information:

- First name
- Last name
- Date of birth
- Residence address (Building, street, city, country)
- Email and/or mobile phone number

Due to the non-face to face customer onboarding nature, the company has implemented mandatory

verification for which tools and technology will be utilized to limit the risk. The company shall reserve the right to block accounts and request alternative documentation should it be deemed necessary.

In order for the company to know it is dealing with a real person, documentation is required at certain intervals to corroborate as much as the information submitted as possible. The company shall obtain sufficient evidence of identity to verify the person is whom they claim to be.

A customer's residential address is an essential part of their identity, and when it is not present on identification documents, it will have to be obtained separately (once the relevant due diligence level is reached).

The KYC will be verified via the KYC provider who will ensure that the documentation provided corresponds to the information currently held on the customer and that the KYC is valid. If the documentation provided is deemed not to be valid or sufficient, further documentation may be requested from the customer.

Following the risk-based approach, at onboarding, a risk assessment of the ML and FT risk posed by the customer is carried out based on the information provided by the customer and checks conducted. The risk assessment will rate the customer as low, medium or high risk. Due diligence and ongoing monitoring will be carried out in proportion to this risk. If the risk is deemed Medium or High, further information and documentation is required from the customer. If the account is rated High Risk and/or is exhibiting trends or there is suspicion, knowledge or reason to believe it must be reviewed by compliance personnel and brought to the attention of the AML Compliance Officer for further investigation.

TIMING OF DUE DILIGENCE

It shall be pertinent that upon request of any documentation and/or information from the customer, a 30-day limit is placed upon the account. During such time, all withdrawals will be blocked until all the necessary information and/or documentation is successfully provided. Failure to provide the requested due diligence will result in the termination of the business relationship.

LEVELS OF DUE DILIGENCE

Due diligence typically involves three main levels: Simplified, Standard and Enhanced. The level of scrutiny applied depends on the risk profile of the customer or transaction. Simplified due diligence is used for low-risk scenarios, while Enhanced due diligence is employed for high-risk cases. Standard due diligence serves as the baseline for most customer interactions.

5.4.1 LEVEL 1 - SIMPLIFIED DUE DILIGENCE (SDD)

The company collects identification information from every customer during the account opening (registration) process, which at a minimum includes – name, address and date of birth. The company also carries out Politically Exposed Persons ("PEP"), adverse media, and sanction screening checks. A customer may only remain on SDD should the risk assessment be a low risk. If following a risk assessment, a customer's risk is deemed to be low, the identification of the customer shall be carried out prior to the establishment of a business relationship. Electronic or bank identification shall be deemed as acceptable means for identification and verification purposes.

In those cases where it is detected that the customer is acting on behalf of, for the sake of clarity, beneficial ownership shall mean any person who is funding the account, hence if a person has an account which is funded by a third party, that third party is considered to be a customer and a beneficial owner. However, such accounts shall be refused by the company.

Such can be detected by:

- Customer requesting to send funds not the original account hence not following closed loop
- Customer is using a payment instrument which does not pertain to the identification documentation held
- Upon review it is identified that the customer is playing on behalf of someone else

If the AML Compliance Officer or any of the AML/CFT team deem that a low-risk customer, due to information available, is likely to threaten the good standing of the AML/CFT function within the company, the customer shall not be considered low-risk. The risk level shall be overridden with justification provided, representing the actual risk level posed by the customer.

5.4.2 LEVEL 2 - CUSTOMER DUE DILIGENCE (CDD)

The company's due diligence procedures deal with identifying customers, understanding their expected product/service usage, and their source of funds and source of wealth. CDD measures based on the customer risk profile and to further substantiate the customer risk profile the following information shall be mandatory assessed:

- Identity verification for every new customer
- Assessing the risk profile of every customer
- Transaction analysis
- Analysis of the historical pattern of the customer's transaction activity
- Surveillance of game play
- Ban of anonymous or fictitious accounts

Customer Due Diligence (CDD) Measures

The company takes measures for CDD:

- When establishing a business relationship (subsists for a period of time);
- At occasional transactions relating to the pay-out of profits or payment of stakes of an amount equal to €2,000 or more; and
- For transactions the amount of which are less €2,000, if the company realizes, or ought to realize, that the transactions relate to one or several other transactions which together amount to at least €2,000.

Identity verification

The company identifies and verifies the customer's identity, and obtains basic customer data (name, personal identity number, registered address, telephone number, e-mail etc.). Also, ensuring that the customer's specified/used bank account or payment method belongs to them.

As the company's customers are non-face-to-face natural persons, the company identifies and verifies their identity remotely:

- Through an established and recognised electronic identification system or equivalent; or
- By retrieving data on the person's name, address, personal identity number or equivalent and verify these data against external records, certificates or other equivalent documentation.

Such which shall be outsourced to a third party provider and if required also have the ID document screened if upon testing suspicion is raised in relation to adequacy of the document. The term outsourced means will provide the technology but all obligations and responsibilities remain with the company.

All customers entering the platform shall be subject to completion of identification including PEP, financial sanction and adverse media checks for which the following is to be obtained:

1. Identity verification
2. Address Verification
3. A selfie

Identity verification of the customer is to be provided as a form of government-issued document/s, such document/s should contain photographic evidence of identity. Acceptable documentation shall be as follows:

- a valid unexpired passport (preferably does not expire in the following six (6) months);
- a valid unexpired national or other government-issued identity card;
- a valid unexpired residence card; or
- a valid unexpired driving license (must hold nationality)

The documentation will be reviewed by a third party provider.

If a customer holds a bank or e-ID such shall be deemed to be sufficient for the identity and address verification.

If there is a suspicion regarding an identification document further documentation is to be requested. Those customers who do not reside within the European Union and reside in a high-risk jurisdiction or where the customer presents a high ML/FT risk, the company shall reserve the right to request further information and documentation pertaining to the customer in order to satisfy any risk or questions related to the identified threat.

Address verification

At this stage (CDD), the customer's address shall also be verified. The address is verified by one of the following documents (which are not more than six months old) that clearly shows the customer's name and residential address:

- A recent utility preferably not older than six (6) months;
- A recent statement preferably not older than (6) months, from a recognised credit institution;
- Correspondence from a central or local government authority, department or agency;
- A record of visit to the address by a senior official of the subject person;
- Any identification document where a clear indication of residential address is provided; or
- Certificate of conduct issued by a law enforcement authority.

In relation to utility bills when verification of a utility bill is done by the company it is to verify that the said document has been issued in relation to the services linked to that residential property. A bill issued in relation to a fixed line telephone service installed on that property would be also acceptable. Mobile telephone bills which are not linked to a fixed premise are not acceptable.

The address verification documents will be uploaded via the provider who will ensure:

- The documents provided are a valid form of Address Verification documentation;
- The documents provided are not more than 6-months old;
- The details provided on the address verification documentation match the customer's account;
- The address verification documentation looks legitimate and not tampered with; and
- The address verification documentation is held on file for a minimum of 5 years.

If a customer holds a bank or e-ID such shall be deemed to be sufficient for the identity and address verification. If there is a suspicion regarding the address verification document further documentation is to be requested.

Those customers who do not reside within the European Union, but reside in a high-risk jurisdiction or where the customer presents a high ML/FT risk, the company shall reserve the right to request further information and documentation pertaining to the customer in order to satisfy any risk or questions related to the identified threat.

The company understands that CDD is a dynamic ongoing process; throughout ongoing monitoring, certain

changes, events or triggers will require the Company to re-complete some or all the CDD measures. The completion of CDD will result in a customer either successfully passing CDD or alternatively being classified as high risk and being immediately subject to EDD.

N.B. if a customer has a change in I.P. of over 90 days, the customer will be prompted to update the proof of address.

5.4.3 LEVEL 3 - ENHANCED DUE DILIGENCE (EDD)

The company applies Enhanced Due Diligence (EDD) measures on a risk sensitive basis in any situation which by its nature can present a higher risk of ML and/or FT, as well as when certain thresholds are reached.

EDD checks include account reviews, adverse media screening, full review of game and transaction history, recording occupation and source of wealth, verification of source of funds and source of wealth, and requests for certified identification documents.

Enhanced Due Diligence ("EDD") Measures

The enhanced measures are supplemented by such additional measures which are required to prevent the high risk of ML/FT, especially for those high-risk customers. At a minimum, the company:

- Retrieves additional information on the customers' financial situation and information on where the customers' financial resources derive from; and
- Gets approval from the relevant senior manager to conclude or cancel a business relationship with the customer, where deemed necessary.

Additional measures implemented by the company include:

- Adverse media checks on the customer through online searches for articles or other relevant information with allegations of criminal activity or terrorism or dealings with criminals or criminal activity.
- Increased frequency for the updating of CDD documentation to ensure that the information is up to date and correct.
- Increased frequency and intensity for reviewing transactions, e.g. that controls must always be made for transactions over certain thresholds (at reasonable levels).

As stated throughout the policy and procedures, EDD is to be applied without delay in instances where the customer is likely to pose a higher than normal ML/FT risk. The AML Compliance Officer and the AML/CFT team are to have a full overview of customers deemed to be of a higher risk.

EDD shall require additional measures concerning where the threat is emanating from, achieved via source of funds and/or wealth requests. The company is to keep all documentation regarding the customer's identity, documentation verification and the risk assessment.

Once EDD has been completed the residual risk is to be adequately assessed in the risk assessment and sufficient ongoing monitoring is to be conducted to address any residual risk. If the residual risk is greater than the company's risk appetite (and cannot be lowered to a satisfactory level by mitigating measures) the account shall be terminated.

EDD verification measures are as follows (note that each will not be required on every EDD verification but based on the information provided by the customer and the risks presented):

- Obtaining additional information and, as is appropriate, substantiating documentation on the intended nature of the business relationship;

- Carrying out additional searches (e.g., internet searches using independent and open sources) to better inform the customer's risk profile;
- Consider the source of wealth and funds involved in the transaction or business relationship to ensure they do not constitute the proceeds of crime. In order to investigate this it could include obtaining appropriate documentation concerning the source of wealth or funds even on the beneficiaries;
- Increasing the frequency and intensity of transaction monitoring; Increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
- Increasing awareness of higher-risk customers and transactions across all departments who have a business relationship with the customer. Increasing awareness also includes the possibility of conducting enhanced briefing with engagement teams responsible for the customer; and
- Obtain Senior Management approval for the continuation of the relationship in cases where the doubt has been raised on approval of the customer.

For high risk customers the system every 12 months or when any transactional triggers are activated will automatically provide an alert on the account. The MLRO can override any risk assessment and therefore be placed on monitoring for which the relationship will be assessed more frequently.

In relation to identification, when the customer is at high risk, or doubts are raised in relation to the identity of the customer, although the customer is registered with electronic or bank identification, a document listed in the verification section is to be obtained.

Information on the economic profile

The following information is obtained at due diligence level 3 to provide information on the profile of a customer.

This information shall be used to further substantiate the business relationship and provide the company with relevant information pertaining to the funds used in the business relationship.

Status of employment:

- a) Retired
- b) Self-employed
- c) Employed
- d) Part-time employment
- e) Student
- f) Unemployed

Proof of income which are risk ranked to reflect the risk of the provenance of the funds as per CRA flow:

- a) Salary income (Low Risk)
- b) Fixed deposit – Savings (Low Risk)
- c) Sale of property (Medium Risk)
- d) Sale of company (Low Risk)
- e) Income from investments (Medium Risk)
- f) Inheritance (medium Risk)
- g) Company profits/ distributed Dividend (Low Risk)
- h) Loan (High Risk)
- i) Crypto investments/ Mining (High Risk)
- j) Funds generated from winnings (Medium Risk)
- k) Pension (Low Risk)
- l) Gift (Medium Risk)
- m) Rental income (MediumRisk)
- n) Gross annual income: A drop down for gross annual income is to be in place, the risk is assessed

depending on the salary brackets for which are likely to increase the risk of ML/FT:

- i) Euro 5,000 - Euro 19,999
- ii) Euro 20,000 - Euro 39,999
- iii) Euro 40,000 – Euro 59,999
- iv) Euro 60,000 – Euro 79,999
- v) Euro 80,000 - Euro 89,999
- vi) Euro 90,000+

A policy review of the account shall be conducted to ensure the customer is properly risk assessed and to corroborate as much of the SOW/F information provided as possible via open source intelligence and research shall be carried out on those customers for which there is a concern in relation to the funding of the account or upon review. If there is a mismatch between the information provided by the customer and background research, this could lead to a ML/FT concern leading to the customer being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

Mandatory Enhanced Due Diligence

EDD will be conducted in the following situations:

- customer is determined to be a high net worth individual who has over two million (2M) Euro in total assets this shall be carried upon review;
- customers with multiple revenue streams from which the provenance of funds is not easily identified;
- customers receiving funds to or from high-risk or non-reputable jurisdictions as per internal jurisdiction risk assessment this shall be carried out upon review of the account;
- customers who are from a high risk or non-reputable jurisdictions as per internal jurisdiction risk assessment;
- customer triggers any of the transactional or fraud triggers shall be temporarily placed on EDD until the situation is rectified and documentation obtained, if not such shall be raised to the MLRO;
- customer deposits more than Euro 10,000 in a 365-day period; and
- customer net losses reached Euro 30,000 in a 365-day period.

Customers at the CDD level shall be rated EDD temporarily until the SOW/F shall be requested if either of the above thresholds are reached. If at the time the above thresholds are reached, the customer is rated as medium risk (CDD), then the customer is only temporarily rated as a High Risk (EDD) until SOW/F is verified, at which point the customer goes back to medium risk (CDD). If the customer's SOW/F is not verified the account is suspended and the customer will remain on the EDD level. If they wish to reactivate the account, the customer will have to provide SOW/F verification documentation.

Should the customer exceed such a threshold, the customer will be prompted to provide the source of funds for the transactions, and a re-evaluation of the customer's profile will be conducted.

We can only request information from the customer which assists us in addressing a concern or understanding how the customer is financing their activity. If a customer refuses to provide any information or fails to provide the necessary information within the relevant time period, we will suspend the account, stop processing any further wagering and shall be effectively blocked. The case shall be raised further with the MLRO to decide whether the case warrants further reporting to the relevant authority by analyzing activity to identify knowledge, suspicion or reason to believe ML/FT.

5.5 ONGOING MONITORING

Ongoing monitoring is an intrinsic part of the due diligence process. It must be performed on all matters, regardless of the risk rating of the customer, to detect unusual or suspicious transactions. The primary objective of ongoing monitoring is to:

- The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds and that the funds are obtained from legitimate lines of business;
- Ensuring that the documents, data or information held by the subject person are kept up to date.
- Keep up-to date information used for CDD or EDD purposes (identity and verification documents, the system will alert those instances where the documentation is about to expire);
- Stay alert to changes in the customer's risk profile and anything that gives rise to suspicion; and
- Monitor transactions for possible indicators of ML/FT.

The company shall examine, as far as reasonably possible, the background and purpose of all transactions that fulfill at least one of the following conditions:

- a. complex transactions that have no apparent economic or visible lawful purpose;
- b. large transactions that have no apparent economic or visible lawful purpose;
- c. unusual patterns of transactions that have no apparent economic or visible lawful purpose; and
- d. transactions which are particularly likely, by their nature, to be related to ML/FT.

A policy review of the account can be conducted at the CDD threshold to ensure the customer is properly assessed. Open source intelligence is also to be used and to corroborate SOW/F information provided this shall be carried out on those customers for which have raised concern in relation to the funding of the account or upon review.

If there is a mismatch between the information provided by the customer and background research, this could lead to a ML/FT concern leading to the customer being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

Ongoing monitoring can trigger a further risk assessment of the customer due to transactional alerts, and if transactions are involved in the alert, they will be scrutinized to establish whether any suspicious activity or transactions are occurring.

A review of the account will be conducted as stated both on the identification and verification information and the transactions. Accounts can have their risk ratings increased via override, such will indicate that the account is to be reviewed more frequently.

Periodic Ongoing Monitoring

Accounts shall be periodically reviewed from the date of the last CRA based on the customer's level of risk:

- High Risk: 12 months (1 year)
- Medium Risk: 24 months (2 years)
- Low risk : 36 months (3 years)

The above time frames are a backstop for when an account review is required. If the customer triggers before and a review is conducted, the periodic review timer restarts and is set from the date of the last customer review.

The company monitors ongoing business relationships and assesses transactions in order to detect activities and transactions that:

- Deviates from what the company has reason to expect based on its customer due diligence,

knowledge of the customer, their business and risk profile.

- Deviates from what the company has reason to expect based on its due diligence of other customers and the products and services, as well as the information provided by the customer and other circumstances.
- Display any unusual patterns of behaviour that may indicate illegal activity.
- Are likely to be part of money laundering and/or financing of terrorism.

Risk factors to be given particular consideration in the monitoring of business relationships and transactions include:

- Gambling or transaction patterns that differ from what is normal or what the customer indicated when the business relationship was established.
- The customer carries out unusually large transactions.
- The customer requests withdrawal to a different account than the account that has been verified to belong to the customer (it is noted that such withdrawals are not possible).
- The customer requests to transfer their gambling account or winnings to someone else (it is noted that such transfers are not possible).

CDD: IP Check

The customer's IP address is registered. Upon registration, a review is done as to whether the customer's IP address corresponds to the registered country. If there is a mismatch, the customer account is marked for further checks.

DD: Double Customer Check

Every customer can open only one account per brand. If a customer tries to open multiple accounts, these will be blocked. The company has measures in place to deter customers from being able to open multiple accounts.

Transaction monitoring

Transaction monitoring shall be based on:

- Automated software (the transactions will be reviewed in real-time);
- Post transaction monitoring the depending on the risk assessment of the customer meaning the review frequency of the account holistically; and
- Triggers, rules and events.

Transaction monitoring is not only determined by the level of risk posed by the customer, but there are also triggers based on (but not limited to) if the customer is exceeding their expected level of activity as determined by the customer's profile IP changes, large or complex transactions and on the rationale behind the activity of the customer.

The company's transaction monitoring is conducted on a risk-based approach under which the intensity of measures preventing ML and/or FT depends on the level and nature of the identified risks. Where a higher risk of ML and/or FT is detected, a more enhanced and focused approach is used and stricter thresholds, rules and measures are implemented. If discrepancies or suspected activities/transactions are noted, the company assesses whether there are reasonable grounds to suspect ML and/or FT or that property otherwise derives from criminal activity.

Employees must report any suspicion of ML and/or FT to the company's MLRO for controlling and reporting obligations. In case of deviation or suspicious activities/transactions, the customer's risk profile is also updated.

Deposit without wagering

It is important to note that due to the current AML/CFT regulations, the customer may deposit money only in order to play and use our services. Therefore, the company adopts a procedure whereby the deposits must be wagered at least once before a withdrawal can be processed.

The company is not a financial institution or credit institution and does not grant interest on deposits. In any case, it reserves the unlimited right to apply certain restrictions to the payment methods if selected.

Trigger events

The compliance function, as part of its ongoing monitoring of business relationships, or when notified or becoming aware of any change in the beneficial ownership pertaining to the customer account is to physically compare beneficial owners, and where suspicion has raised any intermediary or known controlling party against Sanction searches held on the system and physically check them against the following sanction lists:

- <https://main.un.org/securitycouncil/en>
- <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

If such searches reveal a positive match, and the match has met several criteria, such match will be reported accordingly to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Jurisdiction
- Photo identification
- Identification or passport number

If such a match has been found, one should also investigate through open sources to obtain further information and immediately inform the AML Compliance Officer by following internal reporting procedures. The AML Compliance Officer should then investigate any suspicion, knowledge or reason to believe and report where necessary. The AML Compliance Officer shall also have the responsibility of ensuring that the screening is being carried out as instructed.

5.6 REPORTING OF UNUSUAL TRANSACTIONS

Suspicious activity

Suspicious activity is any customer activity that is outside of the ordinary, in other words activity that is not normal or expected activity given the customer's profile. All suspicious activity must be investigated and given due consideration. Therefore, it is crucial that the AML Compliance Officer understands the customer profile, as this understanding is used to determine if there is knowledge, suspicion, or reason to believe that the business or customer is engaging in money laundering or terrorist financing activities.

Any unusual customer activity or transactions that are not commensurate with the established profile of the customer should be considered as a potential indicator of suspicious activity. Following the detection of any potential suspicious activity, the subsequent investigations should establish the reasons for the unusual activity or transaction in order to either eliminate or confirm the suspicion raised. If it is confirmed, the transaction and or the activity must be reported to the AML Compliance Officer as soon as possible. Failure to do so is an offense that could result in immediate relief of duty.

Internal escalation

Customers involved in any form of suspected fraudulent activity, suspicion, knowledge or reason to believe that money laundering or funding or terrorism, funds or any involvement in activities related to terrorism or/ and any suspicious transaction or activity will be reported to the appropriate authorities within the stipulated time frame or immediately upon raise of suspicion. This refers to the illegal depositing of funds obtained from ill-gotten means.

The AML Compliance Officer must determine if the information contained in the report does give rise to a knowledge, reason to believe or suspicion of ML/FT in which case the AML Compliance Officer should proceed to submit a STR/SAR to the FIU in a prompt manner and avoid any unnecessary delays. If there are instances where the request for further information to decide on whether to report, the AML Compliance Officer shall instruct a time frame by which the information is to be received. In instances where the customer does not collaborate or provide further information such is deemed to raise more suspicion, and the report shall be submitted to the FIU accordingly.

External Reporting

The company takes any form of illicit activity very seriously, and any fraudulent activity is strictly prohibited. Fraudulent activity may include, but is not limited to:

- Forgery of documentation;
- Collusion (for which such is not possible at the current stage of operation);
- The use of impermissible software tools to render the customer anonymous;
- The provision of false registration data or other requested information;
- Any red flag identified above.

Where there are suspicion, knowledge or reasonable grounds to suspect that the customer is involved in fraudulent activity, ML/ FT will be reported to the appropriate authorities within the stipulated time frame, which is immediately upon the suspicion being raised. All personnel have direct access to the AML Compliance Officer, and such reports should be raised immediately. The AML Compliance Officer will then be responsible for reviewing the report and to escalate to the relevant FIU accordingly.

Once an STR/SAR has been escalated, it will be included in a STR/SAR central repository within the company. The company shall at all times retain any STR/SAR as follows:

1. Reports raised to the FIU;
2. Reports not raised also hold information on why the report was not raised.

The company may occasionally receive requests for information or notifications from regulatory authorities or law enforcement bodies regarding investigations of a criminal, civil or regulatory nature. When such requests for information are received, these are to be forwarded in their entirety to the company AML Compliance Officer.

The company's AML Compliance Officer will handle and process these requests in line with the following process;

- Record the receipt of such a request;
- Verify the legitimacy of the requesting company and individual making this request;
- Verify the legal basis under which such a request is made;
- Identify the customer account(s) relevant to the request;
- Analyze the customer information, including, amongst others, due diligence, transactions and ongoing monitoring information;
- Re-consider the customer's risk status considering the received request and take appropriate action depending on the case;

- Identify information that is relevant to the request and following a due assessment of the information, prepare and provide the information to the requestor; and
- Update the company records in respect of such a request and where appropriate, notify the relevant regulators or authorities with follow-up actions as per relevant regulatory obligations.

Reporting of suspicious activity or transactions and requests for information shall be sent to the Financial Analysis Unit.

5.7 ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

The AML Compliance Program is a set of policies and procedures implemented to prevent, detect, and report money laundering and terrorist financing.

The Key components of the AML Program consist of:

- **Internal Controls:** This consists of policies and procedures to guide the employee in taking the necessary actions and operations related to AML compliance.
- **Customer Due Diligence (CDD) and Know Your Customer (KYC):** This includes the identification and verification of customers and assess their risk level to prevent criminals from using the company's services.
- **Transaction Monitoring:** This includes the process of monitoring accounts and transactions for any suspicious activity that may indicate money laundering or any other suspicious activity.
- **Employee Training:** This includes internal and external training to all employees to ensure that their roles and responsibilities are clear as able to identify and report any suspicious activity.
- **Reporting:** Internal and External reporting process have been set so that all employees have a clear process for reporting of suspicious activity and take the appropriate steps to report to the authority.
- **Ongoing business risk assessment:** The company's risk exposure is assessed regularly to ensure that the risks exposure is mitigated and remains effective.

An AML compliance program is important to ensure that the company adheres to its regulatory compliance requirements; is mitigating risks to protect from legal, financial and reputational damage that can result from non-compliance; and is contributing to the overall effort to safeguard the global financial system from criminal activity.

7. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Consequences of non-compliance can include financial penalties like fines, legal action ranging from civil lawsuits to criminal charges, and severe operational disruptions such as stopping operations and loss of licenses. Non-compliance also causes reputational damage that can erode customer's trust and negatively affects employee morale and retention.

8. CONTACT INFORMATION

For any questions regarding this policy, please contact us via our email.

9. POLICY HISTORY

Compliance will be continually monitored through any or all of the following methods: file audits; review of records maintained; reports or feedback; and any other method.

We will review this policy at least annually as part of our overall risk management process. We will also review this policy if:

- There are any major changes in the law or practice;
- We identify or are alerted to a weakness in the policy; or
- There are changes in our business, our customers or other changes which impact this policy.