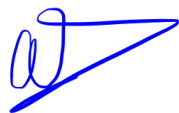


#	Area	Subarea	Control	Control type (prevention/detection)	Procedure description	Frequency / Trigger	Responsible (function)	Execution Method	Reports, backup measures, further actions
1	Customers	Customers registration	Identification Data Collection	prevention	To create a gaming account on the Technology Platform, the player must register at least the following data: i. first name; ii. last name; iii. date of birth; iv. permanent residential address;	covered	Compliance	Automatic control	Account is not opened
2	Customers	Customers verification	KYC Measures	prevention	Verification of the person's identity must include, at a minimum, first name(s), last name(s), type of identification document, identification document number, age and nationality	covered	Support Team, Compliance	Automatic control and manual checks	Player's bets on remote games restricted until the validation process of the registered information and data is completed. Account may be closed without proper verification.
3	Customers	Customers verification	Withdrawal Restrictions Pending Identity Verification	prevention	Registered players may deposit funds into their gaming accounts using payment methods accepted by the operator. However, withdrawals are prohibited until the player's identity and the authenticity of the provided information have been successfully verified.	covered	Support Team	Automatic control	The player's account shall remain locked until the identity verification process has been successfully completed
4	Customers	Customers registration	Single Game Account per Registered Player	prevention	Only players with a unique gaming account, registered in accordance with the provisions of these methodological norms, are permitted to participate in remote games of chance.	covered	Anti-fraud	Automatic control	Multiaccounting is prohibited, any duplicate accounts identified will be closed immediately.
5	Customers	Account closure	Account Closure Due to Unsuccessful Verification	prevention	If a player fails to verify the authenticity of the information provided within 30 calendar days from the date their account is credited, or if the player is identified on a self-exclusion or undesirable players list, the operator shall proceed with account closure.	covered	Support Team, Anti-fraud	Automatic control and manual checks	Upon closure, any remaining funds in the account will be retained in accordance with applicable regulations.
6	Customers	Account closure	Account Closure and Refund in Case of Player's Death	prevention	In the event of a player's death during the verification period, the funds in the account shall be refunded to the lawful successors.	ad hoc	Support Team, Anti-fraud	Manual control	Refunds to the player's successors shall be processed upon presentation of official documentation proving their legal entitlement.
7	Customers	Customers verification	Invalid Documents Detection	detection	If a customer provides invalid information or documentation, the Support Team will make all reasonable efforts to contact the customer and request that they update their profile with valid documents.	covered	Support Team, Compliance	Manual control	Temporary restrictions may be applied to withdrawals and gameplay until valid documentation is received and verified.
8	Customers	Customers verification	PEP Identification and Sanctions List Screening (KYC Procedure)	detection	All players are screened against Politically Exposed Persons (PEP) and international sanctions lists. The Company utilizes third-party solutions and open-source databases to perform these checks.	covered	Support Team, Anti-fraud	Automatic control and manual checks	- Opening of accounts for identified PEPs requires prior approval from the CEO and Directors. - Enhanced Due Diligence (EDD) procedures and ongoing enhanced monitoring are applied to all PEP accounts. - No business relationship shall be established or continued with individuals subject to sanctions.
9	Customers	Customers registration	Country Monitoring and Jurisdictional Restrictions	prevention	Registration from prohibited jurisdictions, as defined in the Company's AML Policy, is blocked.	covered	Compliance	Automatic control	Player accounts originating from prohibited countries cannot be opened.
10	Customers	Customers verification	Enhanced Verification for Risky Players and Based on Country of Residence	detection	Additional verification measures are applied to high-risk players and those whose country of residence mandates enhanced due diligence. These measures include, but are not limited to: - Submission of a photo holding the passport; - Liveness verification; - Sending a password or confirmation code to the registered address - Verification of source of wealth and/or source of funds - Declaration of politically exposed person (PEP) status, including family members or close associates of PEPs	ad hoc	Anti-fraud	Manual control	Operational controls ensure that all verification steps are completed and documented. A comprehensive history of each player's verification and activity is maintained and available for review within the system.
11	Customers	Customers verification	PEP checks by PSPs	detection	Players are screened against PEP lists through integrated checks within each payment system at the time of performing transactions.	covered	Anti-fraud	Automatic control and manual checks	If a match is identified, restrictions may be applied to the account, and a request for additional documentation is sent to the player for further verification.
12	Customers	Player's information	Monitoring of Changes in Player Information	prevention	Changes in registered player information are processed by Support and Anti-Fraud teams. Players are responsible for notifying the operator of any updates to their personal data. Requests to update information must be submitted from the email address used during registration. If discrepancies or inconsistencies are identified through the player's activity, the account is blocked pending verification.	covered	Support Team, Anti-fraud	Manual control	All correspondence with players regarding data changes is documented and reviewed.
13	Payments	Ownership and legality of funds	Credit Card Ownership and Legitimacy of Funds	prevention	Funds deposited via credit card must belong to the player and must be of legal origin. When a deposit is made, the player's identity is matched against the details of the payment method registered in the corresponding payment system. Deposits made by player "A" using a credit card or payment account belonging to player "B" are prohibited.	covered	Payments, Anti-Fraud	Manual control	The prohibition is stated in the Terms and Conditions, which all players must read, accept, and agree to prior to account registration. No manual overrides are technically permitted.

#	Area	Subarea	Control	Control type (prevention/detection)	Procedure description	Frequency / Trigger	Responsible (function)	Execution Method	Reports, backup measures, further actions
14	Payments	Ownership and legality of funds	E-Wallet Deposits – Ownership and Legitimacy of Funds	prevention	Funds deposited via e-wallets must belong to the player and must originate from a legal source. Under the terms of agreements with each payment provider, the responsibility for verifying the legality of funds lies with the respective payment system. Where appropriate, the operator will request information on the player's source of wealth (SoW) and/or source of funds (SoF) as part of the due diligence process.	covered	Support Team, Compliance	Automatic control and manual checks	Formal agreements with payment providers outline their obligations for compliance checks. Additional SoW/SoF verification may be triggered based on risk indicators or transaction patterns.
15	Payments	Monitoring of transactions	Monitoring of Large and Linked Transactions	detection	The Company monitors large or potentially linked transactions that meet or exceed the €2,000 threshold. This includes single transactions or multiple transactions that appear to be connected. In such cases, relevant customer information is reviewed, and an Enhanced Customer Due Diligence (EDD) procedure may be initiated.	covered	Anti-fraud, Support Team, Compliance	Manual control	Transaction and gambling activity limits are applied until the EDD process is successfully completed.
16	Payments	Withdrawal approval	Ownership and Playing History Verification	prevention	Before processing a withdrawal, the Company reviews the player's account ownership information and playing history to ensure consistency and detect any suspicious activity.	ad hoc	Payments	Manual control	
17	Payments	Withdrawal approval	Withdrawal to Original Payment Source	prevention	Withdrawals are only permitted to the original payment method used for depositing funds. The funds in a player's gaming account may be returned solely via the same payment source.	covered	Payments	Manual control	
18	Payments	Withdrawal approval	Requirement of Betting Activity for Deposits and Withdrawals	prevention	Depositing and withdrawing funds without placing bets is strictly prohibited. Player deposits must only be used for their intended purpose - participation in betting activities. Withdrawals will not be permitted unless the player has engaged in betting activity. If no bets have been placed, withdrawal requests require confirmation from the player that their actions comply with applicable legal provisions.	covered	Payments	Manual control	
19	Payments	Withdrawal approval	Automatic and Risk-Based Withdrawal Limits	prevention	Withdrawal limits are automatically set based on the payment system utilized by the player. Additionally, the Company reserves the right to impose withdrawal limits in accordance with its internal risk management policies to mitigate potential risks.	covered	Support Team, Anti-fraud	Automatic control	
20	Payments	Transfer of funds	Prohibition of Financial Transfers Between Player Accounts	prevention	Transfers of funds between different players' gaming accounts are strictly prohibited and technically impossible. Winnings derived from gameplay shall only be paid out to the same payment account used by the player for their deposits.	covered	Payments	Automatic control	
21	Reporting	Reports to Authorities	Suspicious Transaction Report (STR) Submission	detection	Compliance Officer is responsible for submitting Suspicious Transaction Reports (STRs) to the Financial Intelligence Unit (FIU) in accordance with AML legislation. Reports must be filed when objective circumstances related to a business relationship or transaction correspond to indicators of suspicious activity as defined in the AML procedures.	ad hoc	Compliance	Manual control	Following the submission of an STR, employees will comply with all instructions and requests issued by the FIU or other relevant authorities.
22	Data Retention	Players' Data Retention	Record Keeping and Retention of Transaction and CDD Information	prevention	The Company maintains records of all transactions for a minimum of five (5) years. All Customer Due Diligence (CDD) information, including copies of official identification documents (e.g., passports, identity cards, driver's licenses), account files, business correspondence is retained for at least five years following the termination of the business relationship or the date of the occasional transaction.	covered	DPO, Compliance	Automatic control	
23	Fraud	Fraud monitoring	Monitoring of Unusual and Specific Matches	detection	The Company monitors players involved in unusual or specific matches characterized by atypical betting patterns, such as an unusually high volume of bets, significant odds changes in a single region, or large bet amounts. If fraudulent activity is detected, the associated player accounts are blocked.	covered	Anti-fraud	Manual control	Daily reports, including any adjustments or actions taken, are provided to the Head of the Department for review.
24	Fraud	Fraud monitoring	Detection and Investigation of Suspicious Changes in Player Behavior	detection	Any suspicious or unusual changes in a client's behavior are monitored. The playing style of each active player is continuously reviewed to identify common patterns, which are then used to enhance ongoing monitoring efforts. Investigations are conducted as needed, and appropriate communication and corrective actions are taken.	covered	Anti-fraud	Manual control	Correspondence with players is maintained to clarify suspicious activities. If the responsible department identifies risks associated with a player's account, limitations on betting levels may be applied.



5/28/2025

eMagnus Curacao B.V.

Managing Director

