

CAECUS N.V. (163779)

Customer Acceptance Policy

Approved by the Board of Directors



Effective Date: 2 September 2025

Next Review Date: 2 September 2026

1. Statement and Scope of the Policy

Caecus N.V. has adopted this Customer Acceptance Policy to set out clear standards, procedures, and requirements for approving customers on its online gaming and betting platform. The purpose of the policy is to protect the company from being misused for money laundering, terrorist or proliferation financing, sanctions evasion, fraud, and other illicit activities. It also ensures compliance with Curaçao's regulatory framework, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

The policy is aligned with the guidance of the Curaçao Gaming Control Board and forms part of Caecus N.V.'s wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) program. It also reflects internationally recognised standards such as the Financial Action Task Force (FATF) Recommendations, the European Union Anti-Money Laundering Directives.

This policy applies to all directors, officers, employees, contractors, and third parties engaged in onboarding or customer verification processes. No customer is permitted to deposit, withdraw, or place bets on the platform until they have fully met the acceptance criteria and successfully completed all required verification and screening procedures.

This policy applies to every individual or entity seeking to register an account with Caecus N.V., regardless of the channel used. This includes direct registration via the company's official website, mobile applications, affiliate networks, or third-party platforms.

The policy covers the customer relationship from the moment an application is submitted through to account closure or termination. It applies to all products and services offered by Caecus N.V. under its Curaçao gaming licence OGL/2024/1262/0493.

2. Criteria for Accepting Customers

Caecus N.V. only admits customers who fully satisfy all legal, regulatory, and internal compliance obligations. Each applicant must first be verified to confirm they have reached the minimum legal age for gambling, which is eighteen (18) years or higher if required by the laws of their country of residence. Applicants must also provide accurate and verifiable personal information, including their full legal name, date and place of birth, nationality, and current residential address.

The company does not onboard customers who are based in, accessing services from, or conducting transactions in jurisdictions that are restricted under Curaçao's regulations, international sanctions regimes, or Caecus N.V.'s internal list of prohibited countries. As part of the verification process, all applicants are screened against international and domestic sanctions lists, including those issued by the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Sanctions National Ordinance, the Kingdom Sanction Act, and any relevant lists published by the Curaçao Gaming Control Board.

All funds used for betting or gaming must come from lawful and legitimate sources. Where a customer's risk profile requires closer scrutiny, additional documentation may be requested to confirm the source of funds and, where relevant, the source of wealth. Caecus N.V. also reserves the right to deny services to individuals or entities with a known history of fraud, chargebacks, bonus abuse, breaches of gambling regulations, or self-exclusion for problem gambling.

3. Compliance with Curaçao's Legal Framework

Caecus N.V. recognises that its Customer Acceptance Policy is an integral part of the company's wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The policy is designed to operate in full alignment with Curaçao's legislation, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Compliance with these obligations is a core priority across daily operations. Customer acceptance processes are embedded into the company's compliance structure to ensure that due diligence extends beyond onboarding and continues throughout the customer relationship. This allows material changes in a customer's risk profile, behaviour, or jurisdiction to be identified and addressed without delay.

All employees engaged in onboarding and verification are required to complete dedicated training that covers the legislative framework as well as the company's internal policies. Training focuses on applying the Risk-Based Approach effectively, identifying and escalating high-risk indicators, and following proper escalation procedures to the Compliance Officer or senior management.

Caecus N.V. also commissions independent audits at least once a year to evaluate the effectiveness of the Risk-Based Approach and to test the proper implementation of this policy. These audits assess critical processes such as identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD), and the ongoing monitoring of customer activity. Findings are formally presented to the Board of Directors, and any shortcomings are addressed through corrective measures implemented within agreed timelines to ensure continuous compliance and operational integrity.

4. Application of the Risk-Based Approach

Caecus N.V. applies a structured Risk-Based Approach (RBA) during both the onboarding stage and the ongoing assessment of its customers. This approach ensures that the level of due diligence corresponds to the specific risk profile of each customer. The evaluation takes into account multiple risk factors, including the customer's personal and financial background, the type of products and services being accessed, any geographic considerations, and risks linked to the use of particular technologies or channels.

4.1 Assessing the Customer Risk Profile

Caecus N.V. reviews every prospective customer to determine their exposure to risks such as money laundering, terrorist financing, or proliferation financing. This process ensures that the level of due diligence applied corresponds to the customer's individual risk profile.

Low-risk customers

Applicants are classified as low risk when they show a transparent and well-documented source of income, stable employment in sectors considered low risk, and gambling or transaction patterns consistent with their declared financial situation.

Medium-risk customers

Applicants are classified as medium risk when they present some elevated factors, such as income that is legitimate but less straightforward to verify, employment in moderately exposed sectors, or transaction activity showing occasional inconsistencies with their declared profile. These customers are subject to standard CDD with additional verification steps and closer monitoring.

High-risk customers

Customers are deemed high risk if they demonstrate characteristics such as multiple or unclear sources of income, employment in industries with elevated AML risks (for example, cryptocurrency businesses or unregulated financial services), transaction activity inconsistent with their stated income, or if they are identified as Politically Exposed Persons (PEPs), including their family members and close associates. These customers are subject to Enhanced Due Diligence (EDD), which requires more detailed verification, additional documentation, and ongoing monitoring.

Key indicators requiring enhanced scrutiny

- Customers with multiple income sources must provide supporting evidence for each, such as payslips, tax filings, business records, or investment documentation.
- Where income is irregular or inconsistent, for example seasonal or commission-based, customers must submit documents proving the legitimate origin of funds, with ongoing monitoring applied to detect unusual activity.
- PEPs and their close associates are automatically treated as high risk and require comprehensive checks on source of wealth and source of funds, senior management approval before account activation, and continuous monitoring.
- Customers engaging in unusually large or frequent betting must demonstrate that their funds come from legitimate sources, verified through bank statements or income records.

- Disproportionate spending compared to declared income triggers additional checks and supporting documentation.
- Sudden unexplained changes in betting behaviour, especially among casual or tourist players, result in reclassification and enhanced monitoring.
- Attempts to use third parties to deposit, withdraw, or gamble on a customer's behalf are flagged for immediate investigation, with all involved parties subject to verification.
- Operating multiple accounts is treated as suspicious, with linked accounts consolidated and subject to a full review.
- Customers attempting to redeem large amounts of chips without verifiable gambling activity are required to complete identity and source-of-funds verification before processing.
- Customers associated with junket operators are automatically categorised as high risk, with EDD applied to both the customer and the operator, including a review of financial arrangements and funding sources.

Ongoing monitoring

Caecus N.V. regularly monitors customer behaviour to ensure risk profiles remain accurate. Reviews are scheduled on a risk-based basis and are also triggered by material changes, such as unusual transactions, unexplained large deposits, or updated personal or financial details. When a customer's risk level increases, the company applies additional controls, such as EDD, closer transaction monitoring, or restrictions on account activity. This dynamic process ensures that customer risk is managed effectively and remains consistent with regulatory standards.

4.2 Risks Linked to Products, Services, and Transactions

The risk profile of a customer is also shaped by the types of products, services, and transactions they use. Certain activities carry a higher degree of risk because they reduce transparency and traceability. Examples include peer-to-peer transfers, purchasing or exchanging gaming tokens, or funding accounts through anonymous or semi-anonymous methods such as prepaid cards or specific cryptocurrencies.

Accounts that appear to be used primarily for financial transactions rather than genuine gameplay, for example, making large deposits followed by minimal betting before withdrawing funds are subject to additional scrutiny. Similarly, the use of payment instruments not registered in the account holder's name is considered a red flag and requires further verification.

Caecus N.V. actively monitors and mitigates several key risks in this category:

- **Proceeds of crime:** Funds deposited into gaming accounts may originate from criminal activities such as card fraud, narcotics trafficking, or theft. Customers may be required to provide proof of the legitimate origin of their funds, and any transaction suspected of involving criminal proceeds is reported to the Financial Intelligence Unit (FIU).
- **Anonymous payment methods:** The use of prepaid cards, virtual assets, or other anonymous or semi-anonymous funding sources is treated as high risk. Customers using these methods must undergo enhanced verification, with documented evidence of the origin of funds.
- **Improper use of accounts:** Gaming accounts are to be used strictly for gambling activity. Behaviour such as depositing funds, engaging in little or no play, and then withdrawing is prohibited and leads to immediate review, with accounts potentially suspended during investigation.
- **Third-party payments:** If an account is funded using a payment method not registered to the customer, both the account holder and the third party must be identified and verified. The relationship between them must be established and the legitimacy of the funds confirmed.
- **Transfers between accounts:** Transfers between gaming accounts are generally not allowed. Any exceptions must be properly documented, authorised by the Compliance Officer, and retained for audit purposes.
- **Multiple accounts or wallets:** Operating multiple accounts or wallets, even across platforms under Caecus N.V., is considered suspicious. Internal monitoring systems are used to detect and link such accounts to ensure consolidated oversight and review.
- **Frequent changes in payment methods:** Customers who regularly change their bank accounts or payment instruments may be attempting to obscure the source of funds. Such behaviour triggers a detailed profile review and, where necessary, Enhanced Due Diligence (EDD).
- **Identity fraud:** Using stolen personal or financial information to fund accounts poses a significant risk. The company applies robust verification and authenticity checks to prevent this, and suspected cases are reported to the relevant authorities.
- **Electronic wallets:** Certain e-wallet providers may be based in jurisdictions with weak AML/CTF oversight or may allow anonymous cash deposits, making them vulnerable to misuse. Even licensed e-wallets can obscure the final flow of funds when bank statements only show transfers to the wallet without reflecting subsequent transactions. Customers using e-wallets must verify their funding sources, and the provider's licensing and regulatory standards are confirmed before approval.

4.3 Geographic Risk Assessment

Caecus N.V. maintains a geographic risk framework to assess potential risks linked to a customer's location and the origin of their funds. This framework is regularly updated using reliable international sources such as the Financial Action Task Force (FATF) public statements, advisories issued by the Caribbean Financial Action Task Force (CFATF), the European Commission's list of high-risk third countries, the U.S. Office of Foreign Assets Control (OFAC) sanctions lists, the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from sanctioned jurisdictions are not accepted under any circumstances. Clients from high-risk jurisdictions may only be onboarded after completing Enhanced Due Diligence (EDD), which must be approved by senior compliance officers.

A jurisdiction is considered high risk when one or more of the following conditions apply. Countries with weak AML or CFT frameworks, or with poor enforcement of such frameworks, are treated as high risk. Customers from these jurisdictions must provide detailed documentation confirming the source of funds and source of wealth, and their accounts are monitored continuously. Jurisdictions with systemic corruption are also high risk, as they create opportunities for illicit funds to enter the gaming system; in these cases, stricter verification is required, with particular focus on the legitimacy of income. Countries under international sanctions related to terrorism, weapons proliferation, or other criminal activities are generally prohibited, though exceptional cases may be considered with explicit senior management approval and full EDD. Similarly, jurisdictions linked to active terrorist organisations are automatically categorised as high risk, and customers associated with such locations are subjected to enhanced verification, intensive monitoring, and frequent reviews.

To ensure classifications remain accurate, Caecus N.V. consults authoritative sources including FATF's high-risk jurisdiction lists, CFATF statements, the European Commission's AML/CFT deficiency lists, OFAC sanctions lists, the U.S. Department of State's annual reports, and Transparency International's corruption indices, alongside reports on countries supporting terrorist financing or harbouring terrorist groups.

Where a customer's country of residence or funding source appears on a high-risk or sanctioned list, the application is escalated to the Compliance Officer. If onboarding proceeds, EDD measures must be applied. These include comprehensive identity verification, detailed reviews of source of funds and wealth, and ongoing enhanced transaction monitoring for the duration of the relationship.

Risk Indicator	Description	Company Response
Weak AML/CFT systems	Countries with poor or ineffective AML/CFT frameworks or weak enforcement.	Require full documentation of source of funds and wealth; continuous monitoring.
High levels of corruption	Jurisdictions with systemic corruption increasing the risk of illicit funds.	Apply stricter verification, focusing on validating legitimacy of income sources.
International sanctions	Countries under sanctions for terrorism, weapons proliferation, or other illicit activities.	Onboarding prohibited; accounts not accepted.
Terrorist activity	Jurisdictions linked to known terrorist organisations or support networks.	Automatically high risk; apply enhanced verification, strict monitoring, and frequent reviews.
Sanctioned jurisdictions	Countries explicitly listed on sanctions lists.	Onboarding prohibited; accounts not accepted.

4.4 Risks from Channels and Technology

The way customers access Caecus N.V.'s services and the technologies they use can significantly influence their risk profile. Remote onboarding, in particular, carries an increased risk of impersonation or identity fraud. To address these risks, the company employs advanced digital Know Your Customer (KYC) tools, including biometric checks, document authenticity validation, geolocation verification, and multi-factor authentication.

Before introducing any new technologies, payment systems, or platform features, Caecus N.V. carries out a pre-launch risk assessment to ensure they cannot be exploited for money laundering, fraud, or other illicit purposes.

Certain factors are treated with particular caution. Channels that allow customers to remain anonymous are considered high risk. In such cases, enhanced identification and verification measures are applied, including document verification, biometric checks, and real-time

screening against sanctions and Politically Exposed Person (PEP) lists. Remote interaction, although standard in the industry, still requires strict safeguards to reduce impersonation and fraud risks. For this reason, the company applies secure identity verification processes such as biometric validation, liveness detection, and automated document checks during onboarding and transactions.

Additional risk is present when third parties are involved in facilitating customer interactions, especially when the intermediary is not subject to AML or CFT regulations. In such situations, Caecus N.V. performs due diligence on both the customer and the third party. This includes confirming the intermediary's regulatory standing, assessing their AML/CFT framework, and verifying that all information provided is accurate, complete, and reliable.

Risk Factor	Description	Control Measures
Channels allowing anonymity	Access methods that conceal or limit customer identity.	Apply enhanced identification: document checks, biometric verification, and real-time sanctions/PEP screening.
Remote onboarding and interaction	Customers onboarded or transacting present increasing risk of impersonation.	Use biometric validation, liveness detection, document authenticity checks, and multi-factor authentication.
Third-party involvement	Customer interactions facilitated by intermediaries, especially those without AML/CFT obligations.	Conduct due diligence on both customer and third party; confirm intermediary's regulatory status and AML/CFT framework; verify information provided.

4.5 Risk Indicators

Caecus N.V. applies a set of defined risk indicators across several categories to assess the overall risk level of each customer relationship. These indicators form part of the company's Risk-Based Approach (RBA) and ensure that due diligence measures are applied proportionately to the identified level of risk.

The first category relates to the customer's profile. Risk indicators here include multiple or irregular income sources, designation as a Politically Exposed Person (PEP) or close associate, patterns of high or disproportionate spending, sudden increases in spending by

casual players, use of third parties, operation of multiple accounts, redemption of chips without verifiable activity, or links to junket operators.

The second category concerns products, services, and transaction behaviour. Red flags may include signs of criminal proceeds, the use of anonymous or unregulated payment methods, misuse of accounts, reliance on third-party funding, frequent changes in payment instruments, identity fraud, prepaid cards, or multiple e-wallets.

The third category is geographic risk. Customers associated with jurisdictions that have weak AML/CFT systems, high levels of corruption, active sanctions, terrorism connections, or countries flagged by FATF, CFATF, OFAC, or Transparency International's Corruption Perceptions Index are considered higher risk.

The final category is related to channels and technology. Risks arise when customers access services through methods that permit anonymity, register remotely without sufficient verification, or use unregulated third-party intermediaries.

Risk Category	Examples of Red Flags	Due Diligence Measures
Customer Profile	Multiple income sources, irregular earnings, PEP status, disproportionate spending, third-party involvement, multiple accounts, junket associations.	Apply Enhanced Due Diligence (EDD): verify all income sources, conduct source of wealth checks, obtain senior management approval for PEPs, and monitor closely.
Products, Services, and Transactions	Use of anonymous payment methods, proceeds of crime, misuse of accounts, third-party funding, prepaid cards, identity fraud, multiple e-wallets.	Strengthen verification of payment methods, request proof of lawful funds, apply monitoring rules for unusual patterns, and escalate suspicious cases to the FIU.
Geographic	Customers linked to jurisdictions with weak AML/CFT frameworks, corruption, sanctions, or terrorism risks.	Screen against FATF, CFATF, OFAC, EU, and Transparency International lists; apply stricter verification; escalate to compliance for review; refuse service if sanctioned.

Channel and Technology	Anonymous access methods, remote onboarding without robust controls, unregulated third-party intermediaries.	Use biometric and liveness checks, geolocation verification, multi-factor authentication, and conduct due diligence on third parties.
------------------------	--	---

Risk Scoring and Classification

Caecus N.V. uses an internal Risk Calculator that assigns scores to these indicators and aggregates them to determine the customer's risk rating. The risk levels are categorised as follows:

- **Low risk:** Customers with mostly low-risk indicators. Standard Customer Due Diligence (CDD) applies, and documentation is limited to what is legally required or triggered by changes in the customer's profile.
- **Medium risk:** Customers with a mix of low and medium-risk indicators. Standard CDD is supplemented by additional verification and closer ongoing monitoring.
- **High risk:** Customers displaying one or more high-risk indicators. Enhanced Due Diligence (EDD) is required, with senior management approval before onboarding and enhanced monitoring throughout the business relationship.

This scoring framework ensures a consistent, measurable, and proportionate approach to customer due diligence, while also allowing flexibility to escalate cases when new risk factors emerge.

Outcome of Risk Assessment

The overall risk score assigned to a customer determines the depth of due diligence applied. Customers classified as low risk are monitored under standard procedures, while those assessed as high risk are subject to Enhanced Due Diligence (EDD). High-risk cases require senior management approval at the onboarding stage and are monitored on an ongoing basis with heightened scrutiny to identify and respond to any suspicious behaviour throughout the customer relationship.

5. Customer Onboarding Process

Caecus N.V. applies a structured and compliance-focused onboarding process to ensure that only customers who meet the company's acceptance standards are granted access to the platform. No account is activated until the customer has successfully completed all stages of identification, verification, and sanctions screening.

Identification Requirements

During registration, customers are required to provide their full legal name, date and place of birth, nationality, current residential address, and an official identification number, such as a passport or national identity card.

Sanctions and PEP Screening

Every applicant is screened against international sanctions lists and Politically Exposed Person (PEP) databases using automated tools to ensure comprehensive coverage. All alerts or potential matches are reviewed manually by trained compliance staff to confirm accuracy and to eliminate false positives.

Enhanced Checks for High-Risk Customers

If a customer is classified as high risk during the initial assessment, additional verification measures are applied. In such cases, the customer must provide evidence demonstrating the legitimacy of their funds and, where relevant, their source of wealth. Acceptable supporting documents include recent bank statements, business financial records, tax filings, property sale contracts, or investment account statements. These enhanced procedures ensure that all high-risk customers are verified in line with regulatory obligations and internal standards, protecting the company from misuse.

6. Enhanced Due Diligence

Enhanced Due Diligence (EDD) is applied to customers who are assessed as presenting a higher risk profile. This group includes Politically Exposed Persons (PEPs), along with their relatives and close associates, customers residing in or funding accounts from high-risk jurisdictions, individuals engaging in unusually large, complex, or unexplained transactions, and customers whose financial activity does not align with their declared income or business background.

Measures and Verification

EDD requires a deeper level of scrutiny than standard due diligence. The process includes a full review of the customer's source of funds and wealth, supported by credible and independent documentation. It may also involve searches of corporate registries and public records to confirm legal and beneficial ownership, verification of employment or business ownership, assessment of audited financial statements, and detailed checks of adverse media and reputational information from multiple independent sources.

Approval and Oversight

Senior management must approve the onboarding of all high-risk customers. In cases that are particularly complex or sensitive, formal approval by the Board of Directors may also be required.

Monitoring after Onboarding

High-risk customers who are accepted are placed under stricter ongoing monitoring. This includes lower thresholds for triggering transaction reviews, closer scrutiny of transaction behaviour, and more frequent reassessments of their risk profile. These measures ensure that high-risk relationships are managed responsibly, in line with both regulatory requirements and the company's internal risk appetite.

7. Ongoing Monitoring

Caecus N.V. recognises that customer acceptance is not limited to onboarding but requires continuous oversight. Ongoing monitoring ensures that customer activity remains aligned with the profile established at the time of registration and that any irregularities are promptly detected and addressed.

Automated Monitoring of Transactions

The company employs automated monitoring systems designed to identify patterns of unusual or potentially suspicious behaviour. Alerts are generated for activities such as deposits or withdrawals that do not match the customer's declared profile, rapid movement of funds without significant gaming activity, use of multiple or unusual payment methods, or transaction patterns indicative of collusion, chip-dumping, or other prohibited practices. Each alert is reviewed by compliance officers, who analyse the context and decide whether escalation or further investigation is required.

Periodic Reviews and Risk Reassessment

In addition to real-time monitoring, Caecus N.V. performs periodic reviews of customer profiles on a risk-based schedule to ensure that risk classifications remain accurate. If material changes are observed such as relocation to a high-risk jurisdiction, substantial increases in transaction values, or modifications in funding methods - the customer's risk rating is reassessed. Where necessary, enhanced monitoring or additional controls are introduced to mitigate emerging risks.

8. Termination of Customer Relationships

Caecus N.V. reserves the right to suspend or terminate a customer relationship whenever required by regulations, internal policies, or risk considerations. Termination may occur if a customer fails to provide the necessary identification or supporting documentation within thirty calendar days, if activity raises suspicion of money laundering, terrorist financing, or proliferation financing, or if the customer engages in conduct that breaches applicable laws, regulations, or the company's Responsible Gambling Policy.

Handling of Funds and Reporting

If termination is linked to suspected criminal activity, Caecus N.V. promptly files a report with the Financial Intelligence Unit (FIU) in line with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds in the customer's account are returned to the original funding source unless there is a legal requirement to freeze or seize the funds during investigation. Detailed records of all termination actions, including the reasons and supporting evidence, are retained for a minimum of five years.

Circumstances Leading to Refusal or Termination

The company will refuse to onboard or terminate service where customers:

- Are residents of, located in, or transacting from prohibited or sanctioned jurisdictions.
- Fail to provide requested documents or information within the specified timeframe.
- Submit false, misleading, or incomplete information during registration or verification.
- Cannot provide verifiable evidence of legitimate funds or wealth.
- Are involved in, or suspected of, money laundering, terrorist financing, or other criminal activities.
- Are Politically Exposed Persons (PEPs) whose risk profile cannot be sufficiently mitigated.
- Have engaged in fraudulent conduct, bonus abuse, collusion, or other prohibited gambling practices.
- Attempt to transact using third parties without full disclosure and verification.
- Have self-excluded or been excluded for responsible gambling reasons.
- Seek to redeem large chip amounts or withdrawals without verifiable linked gaming activity.
- Are minors or otherwise below the legal gambling age in their jurisdiction.

9. Integration with Responsible Gambling

Caecus N.V. ensures that its Customer Acceptance Policy is fully aligned with the company's Responsible Gambling framework. Protecting customers from gambling-related harm is treated as a central element of the compliance and operational structure.

Indicators of Gambling Harm

If a customer shows signs of potential harm, for example, frequent deposits that appear to exceed their financial capacity or excessively long gaming sessions, the company may take immediate action. Measures may include setting deposit or wagering limits, temporarily suspending the account, or, where necessary, refusing service altogether to safeguard the customer.

Self-Exclusion and Account Restrictions

Any request for self-exclusion is implemented promptly and extended to all accounts connected to the customer to prevent circumvention. These restrictions remain in place for the duration requested by the customer or for as long as required by regulatory guidance.

Staff Awareness and Training

Employees in customer-facing roles receive dedicated training to help them recognise early warning signs of problem gambling. This training is embedded in both the onboarding process and ongoing monitoring so that intervention occurs quickly whenever risk indicators emerge.

10. Record Keeping

Caecus N.V. keeps comprehensive records relating to customer acceptance for a minimum of five years after the termination of a business relationship, in line with applicable regulatory requirements. These records include customer identification and verification documents, proof of address, evidence of source of funds and wealth, transaction monitoring alerts, investigation files, Enhanced Due Diligence (EDD) records, internal compliance reviews, and documentation of account suspensions or terminations.

All records are stored securely in encrypted form and protected with strict access controls to maintain confidentiality and data security. Only authorised personnel may access these records, and all access is logged and periodically reviewed to ensure compliance with internal procedures and data protection standards.

11. Policy Review and Approval

This Customer Acceptance Policy is reviewed at least once every twelve months to ensure that it remains effective, up to date, and compliant with legislation, regulatory guidance, and industry best practices. The review process also considers any changes to the company's risk profile, emerging customer behaviour patterns, and technological developments that could introduce new risks.

Any proposed amendments are prepared by the Compliance Officer and submitted to the Board of Directors for approval before being implemented. All changes are fully documented, and relevant staff are informed and trained to guarantee that the updated policy is applied consistently across all operations.