

NUMERETO B.V. 163869



AML/CTF/CPF POLICY

APPROVED BY THE BOARD OF DIRECTORS



Approval	Review	Compliance Officer	Approval
28/05/2025	28/05/2026	Semen Klyuchyk	The Board of Directors
05/12/2025	05/12/2026	Semen Klyuchyk	The Board of Directors

Contents

1. Statement	2
2. Definitions	3
3. iGaming Landscape Overview	7
4. Assessment of Risks related to Money Laundering, Terrorist Financing and Proliferation Financing	8
4.1. Money Laundering	8
4.2. Terrorist Financing	10
4.3. Proliferation Financing	13
5. Integration of the National Risk Assessment (NRA)	14
5.1. Customer Risk Assessment and Categorization	16
5.2. Ongoing Monitoring	18
6. Risk-Based Approach	19
7. Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) and Client Acceptance Policy (CAP)	22
7.1. Application of Client Due Diligence Measures	23
7.2. Identity Verification and Information Collection	24
7.3. Timing of CDD Measures	24
7.4. Beneficial Ownership and Control Structure Verification	27
8. Transaction Monitoring	27
9. Politically Exposed Persons	30
10. Sanctions Management, FATF, High-risk & License Restrictions	32
11. Suspicious Activity & Transaction Reporting	34
11.1. Examples of Suspicious Activity	35
11.2. Identifying Unusual Transactions	36
11.3. Timely Submission of Reports to FIU	37
11.4. Confidentiality of Suspicious Activity Reporting	37
11.5. Commitment to a Strong Reporting Culture	37
12. Compliance Officer	38
13. Senior Management Responsibilities	40
14. Employee Training and Screening Programme	41
15. Record-Keeping	44
16. AML Compliance Audit	45
17. Regulatory Access and Cooperation	46
18. Internal Audit and Reporting	48
19. Appendices	50
Appendix I (Customer Risk Calculator)	51
Appendix II (Sanctions Policy)	52
Appendix III (Customer Acceptance Policy)	57
Appendix IV (Employee Screening and Monitoring Program	74

1. STATEMENT

NUMERETO B.V. 163869 has established a comprehensive Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) Policy to effectively address the risks of money laundering and terrorism financing. This policy is designed to align with both domestic and international regulatory standards, ensuring full compliance with applicable laws. It serves as a robust framework for managing risks related to client relationships, service offerings, payment systems, geographic operations, and delivery methods.

The Board of Directors (BoD) of NUMERETO B.V. holds ultimate responsibility for approving, implementing, and supervising this AML/CTF/CPF Policy. Regular reviews are conducted annually, with updates implemented when significant regulatory or operational changes occur. In urgent cases, the designated officer may propose revisions based on findings from internal or external AML audits, with careful consideration of associated risks and impacts.

This policy is in strict adherence to the key objectives of Curaçao's AML/CTF/CPF legislative framework. This includes compliance with the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (NOOGH), the National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification when Rendering Services (NOIS), with all amendments effective as of May 16, 2024. Additionally, it adheres to the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

Beyond national regulations, NUMERETO B.V.'s policy incorporates leading international standards and guidelines, including the Financial Action Task Force (FATF) Recommendations, the European Union's Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs), and the Wolfsberg Principles.

The policy is explicitly crafted to meet the supervisory expectations of Curaçao's AML/CTF/CPF regulatory authority, the Curaçao Gaming Control Board. It is mandatory for all directors, officers, employees, and any external consultants engaged in auditing activities to adhere to the principles and procedures outlined in this policy.

2. DEFINITIONS

Alert

A trigger for further review, generated by pre-defined behavioral indicators or transaction patterns that may signal suspicious or illicit financial activity.

Anti-Money Laundering (AML)

A system of internal controls, policies, and practices designed to prevent the concealment of illicit financial proceeds and detect financial crime risks.

AML Policy

NUMERETO B.V.'s internal governance framework for preventing ML/TF, composed of documented procedures, staff training, and audit processes, overseen by the Money Laundering Reporting Officer (MLRO).

AML/CTF/CPF Program

A comprehensive set of procedures implemented to mitigate risks associated with money laundering, terrorist financing, and proliferation financing, maintained under the direction of the MLRO.

Beneficial Owner

The natural person who ultimately owns or controls a customer, despite any intermediaries or account managers.

Blacklist

A list of flagged individuals, organizations, or countries associated with sanctions or other legal restrictions, used as part of compliance screening procedures.

Board of Directors (BoD)

The governing body of NUMERETO B.V., responsible for setting strategic direction and overseeing risk, compliance, and regulatory adherence.

Comprehensive Sanctions

Prohibitive measures imposed by national or international authorities that restrict any form of interaction with specified jurisdictions or entities.

Counter-Proliferation Financing (CPF)

Efforts aimed at stopping the flow of funds used for the development and distribution of weapons of mass destruction.

Counter-Terrorism Financing (CTF)

Regulatory and operational measures to prevent the funding of terrorist organizations and activities.

Criminal Proceeds

Assets obtained, directly or indirectly, as a result of criminal conduct.

Customer

Any natural or legal person who establishes a business relationship with NUMERETO B.V., including through account creation or transactional activity.

Customer Due Diligence (CDD)

The standard process of verifying a customer's identity and assessing their financial background and risk level in accordance with AML/CTF obligations.

Customer Relationship

The ongoing business engagement between NUMERETO B.V. and a customer, from onboarding through to the full lifecycle of service usage.

Due Diligence

An evaluation of legal, financial, and reputational risks before engaging in a business relationship or transaction.

Economic Sanctions

Government-imposed financial restrictions used to influence foreign policy or penalize specific regimes, groups, or individuals.

Egmont Group of FIUs

An international cooperative of Financial Intelligence Units aimed at fostering information exchange and coordinated AML enforcement.

Embargo

A trade ban or restriction imposed by a government on specific countries or products for legal or policy reasons.

Enhanced Due Diligence (EDD)

A deeper level of scrutiny applied to customers deemed high-risk, going beyond standard verification to understand the source and nature of funds.

European Union (EU)

A political and economic union that sets regional AML/CTF standards and publishes official sanctions and high-risk country lists.

Exclusions List

A list of individuals or entities that have been cleared after sanctions or risk screening and are excluded from further compliance actions.

Financial Action Task Force (FATF)

The global intergovernmental body responsible for developing and promoting policies to combat ML, TF, and other threats to the financial system.

Financial Intelligence Unit (FIU)

A national agency tasked with receiving, analyzing, and disseminating suspicious transaction reports (STRs) to law enforcement bodies. In Curaçao, this refers to the FIU as per Article 2 of the Norut.

First Line of Defense

The customer-facing staff responsible for initial KYC verification, data collection, and transaction monitoring, forming the first layer of the compliance structure.

Greylist

A list of jurisdictions identified as having strategic AML/CTF deficiencies but committed to addressing them through corrective actions.

High-Risk Third Country

A jurisdiction recognized by regulators such as the FATF or EU for having insufficient AML/CTF controls, requiring enhanced scrutiny.

Inherent Risk

The baseline level of risk present in a customer or transaction prior to applying any mitigating controls or due diligence procedures.

Investigation

The structured process of examining suspicious transactions or behaviors to determine whether they breach AML/CTF regulations or internal policy.

Know Your Business (KYB)

Due diligence measures aimed at corporate clients to verify ownership structure, business legitimacy, and regulatory status.

Know Your Customer (KYC)

Procedures used to identify and verify the identity of a customer, assess their financial behavior, and detect potential risk indicators.

Know Your Employee (KYE)

Internal vetting processes to assess employee integrity and identify potential internal threats, including conflicts of interest or criminal background.

Layering

The second phase of money laundering, involving complex financial transactions to obscure the origin of illicit funds.

Minor

An individual below the legal age of 18.

Monitoring

The continuous observation of customer behavior and transactions to identify anomalies that may suggest ML/TF activity.

Money Laundering

The process of disguising the origin of funds obtained through criminal activity. It typically includes placement, layering, and integration.

Money Laundering Reporting Officer (MLRO)

The individual appointed to oversee NUMERETO B.V.'s AML framework, handle internal alerts, and submit Suspicious Transaction Reports (STRs) to the FIU.

National Ordinance on Offshore Games of Hazard (NOOGH)

Curaçao's legislative framework regulating offshore gaming operations and establishing AML/CTF responsibilities for license holders.

Office of Foreign Assets Control (OFAC)

A U.S. Treasury Department agency responsible for enforcing economic and trade sanctions based on national security and foreign policy concerns.

PEP – Politically Exposed Person

An individual holding a prominent public position or government role, whose financial activity requires enhanced scrutiny due to increased corruption risk.

Red Flag

A warning indicator of potentially suspicious activity that requires further review or escalation within the compliance framework.

Regulatory Agency

A government or independent authority responsible for enforcing financial regulations and overseeing licensed institutions.

Sanctions List (Mandatory)

An official compilation of restricted parties such as those maintained by the UN, EU, OFAC that regulated entities must check during onboarding and transaction processing.

SAR/STR – Suspicious Activity/Transaction Report

A report submitted to the FIU when there is reasonable suspicion that a transaction may be related to money laundering or terrorist financing.

Source of Funds / Source of Wealth (SOF/SOW)

Information provided by the customer to demonstrate the origin of their assets or income, used to assess financial legitimacy and risk level.

UK – United Kingdom

A jurisdiction with established AML/CTF standards and a global influence in financial regulation.

UN – United Nations

An international body whose Security Council issues binding sanctions lists that must be adhered to by member states.

US – United States

A jurisdiction with extensive AML enforcement protocols and sanctions systems affecting international financial relationships.

3. iGAMING LANDSCAPE OVERVIEW

NUMERETO B.V. 163869 is a legally registered entity in Curaçao and is the operator of the website <https://rolsbet.com/en>. The company conducts its activities under an official online gaming license issued by the Curaçao Gaming Control Board (License No. OGL/2024/315/0489). This license enables NUMERETO B.V. to operate within the legal framework established by Curaçao's regulatory authorities, which enforce strict licensing requirements and territorial restrictions.

As per these regulatory requirements, the company is prohibited from providing online gaming services in jurisdictions where such activities are restricted. Specifically, NUMERETO B.V. does not offer or promote its services in the United States, Australia, the Dutch West Indies (including Aruba and Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. By adhering to these restrictions, NUMERETO B.V. ensures its operations remain confined to regions where online gaming is legally permitted and actively avoids targeting or marketing to customers in prohibited jurisdictions. This demonstrates the company's commitment to full compliance with applicable legal and regulatory obligations.

The online gaming and betting industry, including companies like NUMERETO B.V., operates in a dynamic environment with inherent risks associated with money laundering and financial crime. These risks include, but are not limited to:

1. Identity Theft: Criminals may use stolen identities or fraudulent accounts to conceal the origins of illicit funds and integrate them into legitimate financial systems through online gaming platforms.
2. Fraudulent Activities: Fraud may manifest in various forms, including credit card fraud, account hacking, or the use of synthetic identities to manipulate gaming systems and bypass safeguards.

3. Structuring and Layering: These techniques involve breaking down large amounts of illicit money into smaller, less conspicuous transactions or disguising the source of funds through multiple layers of transactions to evade detection.
4. Collusion and Internal Threats: Collusion between employees, customers, or third-party payment providers presents a significant risk. Malicious actors may work together to circumvent internal security protocols, enabling money laundering schemes to go undetected.
5. Use of External Payment Providers: Fraudulent activities can also involve external payment processors, e-wallets, or cryptocurrency platforms, which may be exploited to facilitate untraceable transfers of illicit funds.

Given the complexity of these risks, NUMERETO B.V. has established robust policies and controls to identify, mitigate, and address potential vulnerabilities. The company employs advanced monitoring systems, conducts thorough customer due diligence (CDD), and ensures ongoing transaction monitoring to detect unusual or suspicious activities. Additionally, employee training programs are implemented to enhance awareness and equip staff with the skills to identify and respond effectively to financial crime risks.

By maintaining these stringent measures, NUMERETO B.V. underscores its commitment to operating within a secure and compliant framework, safeguarding its customers, business reputation, and the broader integrity of the online gaming industry.

4. ASSESSMENT OF RISKS RELATED TO MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

4.1. Money Laundering

Money laundering is a central component of financially driven criminal activities, often involving complex schemes that span multiple jurisdictions. It facilitates a range of illegal activities, including but not limited to tax evasion, fraud, sanctions violations, corruption, illegal arms trading, drug trafficking, extortion, and human trafficking. The primary objective of money laundering is to obscure the illicit origins of criminal proceeds by concealing their identity, source, and destination, ultimately integrating them into the legitimate financial system.

The Key Stages of Money Laundering

Money laundering typically progresses through three distinct stages, each designed to make tracing illicit funds increasingly difficult:

1. Placement:

This initial phase involves introducing illegally obtained funds into the financial system. Common methods include depositing cash into bank accounts, purchasing high-value assets such as vehicles, jewelry, or real estate, or using other financial instruments to legitimize the money. The goal is to initiate the process of blending illicit funds with legal financial activities to reduce the risk of detection.

2. Layering:

At this stage, the focus shifts to creating a complex web of financial transactions to obscure the money's origins. Techniques include transferring funds across multiple accounts, jurisdictions, or financial institutions, converting them into different currencies, or investing in assets or financial products. This complexity is designed to break the audit trail, making it increasingly difficult for authorities to trace the funds back to their illegal source.

3. Integration:

In the final stage, the laundered funds are reintroduced into the legitimate economy. This is typically achieved through the purchase of luxury items, investments in businesses, or participation in other lawful financial activities. By this point, the funds appear to be legitimate, significantly reducing the chances of detection and recovery.

Money laundering schemes can utilize any of these stages, and online gambling platforms are particularly vulnerable to exploitation due to their virtual nature, high transaction volumes, and international reach. To address these vulnerabilities, NUMERETO B.V. avoids offering anonymous services and closely monitors for suspicious transactions.

Relation to Terrorist Financing (TF)

Terrorist financing, while distinct from money laundering, shares similar mechanisms for moving and disguising funds. These funds may originate from legitimate sources, such as donations or business operations, or from illegal activities like drug trafficking or extortion. Regardless of the source, terrorist financiers use methods resembling money laundering to integrate the funds into financial systems while masking their ultimate destination.

For example, prepaid cards are a common tool used by terrorists to acquire materials or fund operations while maintaining anonymity. Recognizing this overlap, NUMERETO B.V. ensures its staff remains informed about emerging trends in terrorist financing and receives regular training to identify and respond to suspicious activities effectively.

Risk Management and Compliance Measures

To mitigate risks related to money laundering and terrorist financing, NUMERETO B.V. employs a proactive, multi-faceted risk management approach that includes:

1. **Verification of Customer Identity and Fraud Prevention:**
The company conducts comprehensive customer due diligence (CDD), verifying the identity, age, and location of its customers through reliable documentation. Enhanced due diligence (EDD) is applied to high-risk customers, such as politically exposed persons (PEPs).
2. **Detection of High-Risk Transactions:**
NUMERETO B.V. actively monitors for unusual activities, such as the operation of multiple accounts by a single user or unusually large or frequent transaction volumes that may signal attempts at structuring or layering.
3. **Prevention of Illicit Deposits:**
The company identifies and investigates funds suspected of originating from criminal activities or attempts to use the platform as a temporary holding space for such funds.
4. **Monitoring of Player-to-Player Transfers:**
Platforms that enable player-to-player transactions are particularly vulnerable to misuse for money laundering. NUMERETO B.V. implements controls to detect and prevent these activities, ensuring that funds are not transferred illicitly or withdrawn without proper scrutiny.
5. **Ongoing Risk Assessments and Training:**
Recognizing that money laundering risks evolve constantly, the company conducts regular, tailored risk assessments to address emerging threats. Employees receive ongoing training to stay updated on AML compliance best practices, ensuring vigilance across all levels of the organization.

This approach enables NUMERETO B.V. to proactively address existing and emerging threats, reinforcing its commitment to compliance and safeguarding the integrity of its operations and the broader financial ecosystem.

4.2. Terrorist Financing

Terrorist financing refers to the provision and management of funds to support terrorist activities, ranging from minor operations to large-scale attacks. These funds are indispensable for carrying out a variety of operations, including recruitment, training, procurement of weapons, and execution of attacks. The sources of such funds can stem from both legitimate and illegitimate activities, making their detection and prevention particularly challenging.

Sources of Terrorist Financing

1. **Legal Sources:**
Funds from legal sources often derive from legitimate businesses, charitable donations, and other lawful financial activities. Terrorists may exploit these

channels by masking illicit intentions within routine transactions. For example, charitable organizations and fundraising efforts can be manipulated to redirect donations toward financing terrorist operations. Similarly, businesses may be used as fronts to generate and funnel funds under the guise of legitimate activities.

2. **Illegal Sources:**

Illegal sources of funds involve a broad spectrum of criminal activities, including drug trafficking, fraud, smuggling, extortion, and other organized crimes. These illicit gains are often laundered to obscure their origins before being used to support terrorist activities. This convergence of money laundering and terrorist financing underscores the need for vigilant financial oversight and regulatory compliance.

Methods of Transferring Funds

The transfer of funds for terrorist purposes occurs through both formal and informal channels, each presenting unique challenges:

1. **Formal Channels:**

Traditional banking systems and financial institutions are often used to transfer funds. Advanced money laundering techniques such as layering, structuring, and the use of shell accounts can disguise the origins and destinations of these transactions. Sophisticated technology and global connectivity further complicate the task of tracing funds within formal financial networks.

2. **Informal Channels:**

Informal methods, such as hawala systems and other alternative remittance networks, operate outside conventional banking frameworks. These systems rely on trust-based mechanisms and lack standardized documentation, making them difficult to monitor and regulate. Such informal networks are frequently exploited to transfer funds quickly and anonymously across borders.

Indicators of Terrorist Financing

Detecting terrorist financing often requires analyzing unusual transaction patterns or behaviors that deviate from expected norms. Common red flags include:

- Large or frequent fund transfers to or from jurisdictions classified as high-risk or conflict zones.
- Transactions linked to individuals or entities associated with known terrorist organizations.
- Suspicious activities in high-risk industries, such as charitable organizations, where funds may be misappropriated.

- Large deposits or withdrawals that lack a clear business or personal justification.
- Financial activities that appear deliberately structured to obscure their true purpose or circumvent regulatory scrutiny.

Measures to Combat Terrorist Financing

NUMERETO B.V. has established rigorous Anti-Money Laundering (AML) policies to address and mitigate the risks of terrorist financing. These policies focus on:

1. Customer Due Diligence (CDD):
Comprehensive procedures are in place to verify customer identities, assess the risk profile of clients, and ensure ongoing monitoring of their financial activities.
2. Transaction Monitoring:
Automated systems are employed to detect unusual or suspicious transactions, with additional scrutiny applied to high-risk areas and individuals.
3. Sanctions Screening:
The company adheres to multiple international sanctions lists to ensure compliance and prevent financial support for terrorist organizations. These lists include but are not limited to:
 - Sanctions National Ordinance (SNO)
 - Kingdom Sanction Act
 - Curaçao Gaming Control Board (GCB) announcements
 - Office of Foreign Assets Control (OFAC) and its Specially Designated Nationals (SDN) list
 - United Nations Security Council sanctions
 - European Union (EU) sanctions
 - United States Foreign Terrorist Organizations list

NUMERETO B.V. actively uses these sanctions lists to screen transactions and ensure no financial interactions inadvertently support terrorism.

International Framework and Guidelines

Global efforts to combat terrorist financing are guided by international organizations and regulatory frameworks:

1. Financial Action Task Force (FATF):
The FATF provides a set of international standards and recommendations aimed at combating money laundering and terrorist financing. Its guidelines emphasize robust measures for identifying, reporting, and mitigating suspicious transactions.

2. Office of Foreign Assets Control (OFAC):
OFAC enforces U.S. economic and trade sanctions while maintaining the SDN list. This list identifies individuals and entities linked to terrorism and restricts their access to the financial system.
3. European Union (EU):
The EU enforces strict regulations to prevent the misuse of the financial system for terrorist purposes. Member states are required to implement effective AML measures and comply with international sanctions.
4. United Nations (UN):
The UN plays a pivotal role by imposing sanctions on entities and individuals linked to terrorism. Its global sanctions lists are critical in disrupting the financial networks of terrorist organizations and limiting their resources.

By implementing these measures and adhering to international best practices, NUMERETO B.V. demonstrates its unwavering commitment to preventing terrorist financing and maintaining the integrity of its financial and operational systems. Continuous employee training and regular risk assessments further enhance the company's ability to detect and address emerging threats effectively.

4.3. Proliferation Financing

NUMERETO B.V. recognizes the critical importance of addressing Proliferation Financing (PF), which involves the use of financial resources to support the development, acquisition, transfer, or delivery of weapons of mass destruction (WMD) and their associated delivery systems. In accordance with the updated Curaçao iGaming regulations, NUMERETO B.V. has implemented robust measures to ensure its platform is not misused for PF-related activities. These measures include conducting thorough risk assessments to identify and mitigate PF risks, applying enhanced due diligence (EDD) to customers or transactions from high-risk jurisdictions, and monitoring for unusual transaction patterns linked to sanctioned entities or activities.

The company adheres strictly to international sanctions regimes, including those enforced by the United Nations Security Council and the European Union, as well as Curaçao's national legislative requirements under the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act. Transactions and counterparties are routinely screened against relevant sanctions lists to ensure compliance and prevent any financial interaction that could facilitate WMD proliferation. By integrating these controls into its AML compliance program, NUMERETO B.V. underscores its commitment to global non-proliferation efforts while maintaining the integrity and security of its operations.

5. INTEGRATION OF THE NATIONAL RISK ASSESSMENT (NRA)

NUMERETO B.V. upholds a robust AML/CTF/CPF compliance framework that safeguards its gaming services, operations, and financial channels against misuse for money laundering, terrorist financing, or proliferation financing. This framework is built in accordance with the laws and regulations of Curaçao, incorporates the expectations of regulatory authorities including the Curaçao Gaming Control Board (GCB), and aligns with the international standards set by the Financial Action Task Force (FATF) and the Caribbean FATF (CFATF). All internal and external stakeholders employees, executive leadership, business partners, and service providers are expected to adhere to this framework in the course of their operational responsibilities.

Governance and Oversight

The Board of Directors at NUMERETO B.V. is ultimately accountable for the establishment, effectiveness, and continuous improvement of the company's AML/CTF/CPF compliance program. The Board ensures the allocation of sufficient resources, technological capabilities, and qualified personnel to manage the specific risks associated with online gambling. Senior Management supports this mandate by executing operational controls, fostering a risk-aware culture, and granting the Compliance Officer unrestricted access to systems, data, and records necessary to fulfill their duties.

Compliance Officer's Role and NRA Integration

The designated Compliance Officer manages the implementation and daily operations of the AML/CTF/CPF program. This includes oversight of client due diligence (CDD and EDD), transaction monitoring, suspicious activity reporting, internal investigations, and direct liaison with the FIU Curaçao and other competent authorities. In line with AML Regulation III.1, the Compliance Officer ensures that the company's internal controls reflect national and international risk developments.

NUMERETO B.V. integrates the findings of the most recent **Curaçao National Risk Assessment (NRA)** into its enterprise-wide risk framework to ensure consistency with the nationally recognized threats and vulnerabilities. The Compliance Officer regularly reviews NRA publications and assesses their implications for the company's client profiles, product offerings, payment channels, business jurisdictions, and use of financial technologies.

Application of NRA Findings

Insights from the NRA directly inform the Institutional Risk Assessment and are used to shape the company's risk-based approach across its AML/CTF processes. In

particular, the Company makes necessary adjustments in areas identified as high-risk, including but not limited to:

- Strengthening identity verification procedures.
- Raising transaction monitoring thresholds.
- Applying more restrictive controls on specific jurisdictions or payment mechanisms.
- Introducing surveillance rules to counter evolving typologies highlighted in the NRA.

Whenever new risks or emerging threats are identified in the NRA, the Compliance Officer assesses whether current controls are adequate or require enhancement.

CDD and EDD Measures Guided by NRA

NUMERETO B.V. enforces strict Know Your Customer (KYC) protocols before withdrawals or when players meet designated risk or value thresholds. Identity, age, payment method ownership, and residence verification are all integral components of the CDD process. When risk indicators arise particularly those reflecting NRA-referenced vulnerabilities enhanced due diligence (EDD) procedures are applied. EDD may include obtaining:

- Source of funds and wealth documentation,
- Negative news screenings,
- Senior Management approval before relationship continuation.

These measures apply to high-risk jurisdictions, politically exposed persons (PEPs), VIP/high-value clients, and clients with complex transactional behavior.

Ongoing Monitoring and Reporting

The company uses a combination of automated monitoring systems and manual controls to continuously review client activities. The scope of monitoring includes deposit frequency, wagering anomalies, rapid betting patterns, device and IP data, and bonus or account abuse indicators. Alerts are generated in real-time and escalated to the Compliance Officer for prompt analysis and action.

All Unusual Transaction Reports (UTRs) and Suspicious Transaction Reports (STRs) are submitted to FIU Curaçao in compliance with NORUT and AML Regulation IV.1. Employees are instructed to escalate red flags without delay and maintain strict

confidentiality. Tipping-off is explicitly prohibited and may lead to disciplinary action or legal consequences.

Recordkeeping and Training

NUMERETO B.V. ensures all records including CDD data, transaction logs, monitoring results, internal reviews, and NRA-related documentation are retained for at least five (5) years. The company delivers regular AML/CTF training, including updates on NRA findings, legal obligations, and typologies affecting the gambling sector. The AML/CTF framework is reviewed annually and updated as required, based on national developments, regulatory feedback, or industry-wide technological changes.

5.1. Customer Risk Assessment and Categorization

NUMERETO B.V. evaluates money laundering (ML) and terrorist financing (TF) risks by applying a structured client risk scoring system. The system is based on various criteria, including client behavior, transactional patterns, geographic risk, and other red flags. This enables the company to manage risk proportionately and apply the appropriate level of due diligence and monitoring.

The weight assigned to each risk criterion determines the client's total risk score and the corresponding due diligence requirements:

Category	Score Range	Due Diligence Level	Approval Required
Low Risk	0 – 1.8	Standard Due Diligence	Client Service / Compliance Officer
Medium Risk	1.8 – 2.5	Standard Due Diligence	Client Service / Compliance Officer
High Risk	2.5 or more	Enhanced Due Diligence	Compliance Officer approval + annual review
Unacceptable	Qualifying factors	Rejected outright	Automatically rejected

Risk scoring dictates how each client is treated in terms of verification, data collection, and transaction monitoring. Regardless of category, NUMERETO B.V. screens all clients against PEP, sanctions, and adverse media lists as part of the onboarding and ongoing monitoring process. For more details, please refer to **Appendix I**.

Treatment Based on Risk Categories

Low Risk

Clients in this category are considered to pose minimal risk; however, due to the high-risk nature of the online gambling industry, Simplified Due Diligence (SDD) is not applied. Standard Due Diligence (SDD) is performed.

Medium Risk

Clients in this group may present moderate risk, which requires close scrutiny through standard CDD processes. Periodic reviews are conducted to ensure continued compliance.

High Risk

Clients falling into this category require Enhanced Due Diligence (EDD). Approval by the Compliance Officer is mandatory before establishing or continuing the relationship. High-risk clients may include those who:

- Operate in unusual or complex business structures.
- Conduct transactions that are inconsistent with their profile or that of their peer group.
- Are residents of high-risk or sanctioned jurisdictions.
- Are identified as Politically Exposed Persons (PEPs), their family members, or close associates.
- Receive high-risk scores based on onboarding assessments or cumulative behavior (e.g. adverse media, large or irregular deposits).
- Provide suspicious or unverifiable identification documentation.
- Are involved in transactions lacking clear legal or economic rationale.
- Represent companies providing financial services or handling funds for third parties.
- Have total deposits exceeding high-risk thresholds during the business relationship.

Unacceptable Clients

NUMERETO B.V. automatically rejects any business relationship involving:

- Persons or entities subject to international or domestic financial sanctions.
- Individuals engaged in money laundering or terrorist financing activities.
- Minors under the age of 18.

- Individuals with unverifiable or suspicious sources of wealth or funds.
- Customers exhibiting transaction patterns that align with known fraudulent schemes.

NUMERETO B.V. upholds a strict risk appetite aligned with its regulatory obligations and internal controls. The company avoids onboarding clients whose profiles are incompatible with its compliance framework, and all client risk classifications are recorded, justified, and periodically reassessed.

5.2. Ongoing Monitoring

Numereto B.V. is committed to the continuous oversight of its customer relationships in accordance with its risk-based approach and obligations under AML/CTF/CPF regulations. Ongoing monitoring ensures that customer profiles remain accurate, that due diligence remains current, and that unusual or suspicious activity is promptly identified and escalated.

Regular Screening Activities

The Compliance Team conducts regular screening of customers against Politically Exposed Persons (PEP) databases, international sanctions lists, and adverse media sources. Any alerts that result in true matches are subject to escalation and may trigger an event-driven review.

Event-Driven Reviews

Certain events or triggers may require a reassessment of the customer's risk status and, where applicable, a full refresh of due diligence records. These events include, but are not limited to:

- The discovery of new information that calls into question the accuracy or completeness of the previously obtained CDD data.
- The emergence of suspicious behavior or transactional activity.
- A significant change in the customer's risk profile.

In such cases, Numereto B.V. performs immediate and comprehensive reassessments, regardless of the customer's existing risk classification.

Periodic Reviews

Numereto B.V. ensures that customer information is accurate and up to date by conducting scheduled periodic reviews. These reviews are risk-based and follow a structured frequency:

- **High-Risk Customers:** Reviewed annually. This includes re-confirmation of address, updated information on source of funds and source of wealth,

screening for adverse media, and a complete reassessment of transaction patterns and product usage.

- **Medium-Risk Customers:** Reviewed every two years. The review process includes confirmation of address, verification of financial background, adverse media screening, and a general review of account behavior.
- **Low-Risk Customers:** Reviewed every three years, unless a trigger event occurs. These reviews involve verification of address and screening for negative news, with the objective of determining whether the low-risk classification remains appropriate.

Trigger events that may prompt an unscheduled review include:

- Information that undermines the reliability of existing CDD records.
- Identification of activities or patterns that deviate from the expected behavior.
- Regulatory or institutional developments requiring immediate reassessment.

NRA-Based Adjustments

Monitoring procedures are periodically reassessed in line with updates to the National Risk Assessment (NRA). Any changes to national risk priorities are reflected in the Company's internal controls, transaction monitoring strategies, and customer review protocols. This ensures that Numereto B.V. maintains an adaptive and responsive AML framework aligned with both regulatory and sectoral risk developments.

6. RISK-BASED APPROACH

Numereto B.V. adopts a comprehensive risk-based approach to detect, manage, and mitigate the potential use of its online gaming platform for money laundering, terrorist financing, and proliferation financing. This methodology is grounded in the Financial Action Task Force's guidance on risk assessments and integrates both qualitative and quantitative analysis of risk elements such as threats, vulnerabilities, controls, and possible impact across all operational areas.

The company conducts a formal Business Risk Assessment (BRA) on an annual basis and whenever material changes occur in its operational model, regulatory framework, or product offerings. This assessment is formally documented, approved by the Board of Directors, and updated when necessary to reflect evolving risks or new supervisory expectations.

Client Risk

Clients represent a primary risk channel in any AML/CFT framework. Numereto B.V. assesses customer-related risks by evaluating various indicators, such as the complexity of the client's financial profile, inconsistencies in spending behavior, or connections to higher-risk jurisdictions. Politically Exposed Persons (PEPs), individuals with complex income structures, or those showing significant discrepancies between declared income and transaction behavior are subject to enhanced scrutiny.

Clients with low-risk profiles typically display a single, documented source of income and consistent transactional behavior. In contrast, those with irregular deposits, complex fund sources, or high-volume activity undergo enhanced due diligence and closer monitoring.

Product, Service, and Transaction Risk

Certain financial instruments and gaming services pose heightened exposure to financial crime. Numereto B.V. identifies risks associated with digital wallets, cryptocurrencies, prepaid instruments, and peer-to-peer transfers, particularly when used to disguise the origin of funds.

To mitigate these risks, the company applies transaction limits, conducts real-time monitoring, and configures automated alerts to flag atypical behavior such as unusually large wagers, rapid cycling of funds, and account activity inconsistent with the customer's profile.

Geographical Risk

The jurisdictional exposure of clients is a key element in the risk assessment. Clients operating from or linked to countries with weak AML/CFT regimes, high corruption indices, or targeted by international sanctions are considered high-risk.

To classify geographical risk, Numereto B.V. relies on publicly available data and intelligence from sources including FATF, CFATF, the European Commission, OFAC, the US State Department, and Transparency International. Enhanced controls, including restrictions or enhanced due diligence, are applied to clients or transactions linked to such jurisdictions.

Distribution Channel Risk

The nature of the interaction between the client and the company also contributes to the risk profile. Remote onboarding channels, particularly those that do not include face-to-face interaction, may increase the chance of identity fraud or misuse.

To mitigate this, Numereto B.V. uses robust identification systems including digital identity verification, biometric tools, and authentication protocols. Client due diligence

is applied uniformly across all channels, ensuring that no platform remains a weak point in the compliance framework.

Technological Development Risk

Before implementing any new technology or introducing major changes to digital infrastructure, Numereto B.V. conducts a formal and documented technological risk assessment. This includes a written evaluation of the product or process, identified vulnerabilities, proposed mitigation strategies, and residual risk ratings.

Such assessments are carried out for new gaming platforms, payment technologies, use of AI or blockchain, and other innovations that could change the company's exposure to financial crime. The assessments are stored in compliance records and made available to the Gaming Control Board upon request.

Sector-Specific Risk in Online Gaming

As an operator in the iGaming sector, Numereto B.V. recognizes the sector's particular vulnerabilities to money laundering. Criminal actors may exploit rapid transaction flows, irregular betting patterns, or bonus abuse schemes to clean illicit proceeds.

To prevent this, the company prohibits the use of anonymous payment methods, requires that all financial flows pass through licensed institutions, and screens for manipulation attempts such as gameplay matching or excessive bet recycling.

Mitigation and Monitoring

Identified risks are addressed through tailored control measures. These include applying enhanced due diligence, collecting additional documentation, implementing account restrictions, and ensuring automated and manual transaction monitoring systems are actively detecting red flags.

Clients and Payment Service Providers are assessed during onboarding and reassessed during their relationship with the company, with a clear allocation of risk profiles ranging from low to high. Screening is continuous, including adverse media checks, sanctions screening, and PEP status updates.

Recordkeeping and Reporting

All records relating to risk assessments, client profiling, and monitoring results are securely retained in accordance with applicable legal requirements and are made available to the regulator upon request. Suspicious activity is reported promptly to the Financial Intelligence Unit, and tipping-off is strictly prohibited.

Governance and Accessibility

Numereto B.V. maintains structured and evidence-based BRA and CRA documentation. These documents evaluate inherent and residual risks across products, services, clients, and jurisdictions, and are updated regularly. Both the BRA and CRA are retained in formal records and made available without delay to the Gaming Control Board or any other competent authority when requested.

7. CLIENT DUE DILIGENCE (CDD), ENHANCED DUE DILIGENCE (EDD) AND CLIENT ACCEPTANCE POLICY (CAP)

When initiating a business relationship with new clients, NUMERETO B.V. is required to assess whether a client presents any risks related to money laundering, terrorist financing, or proliferation financing that could compromise the integrity of the platform. The client due diligence (CDD) process serves as the foundation for the risk-based assessment by evaluating indicators of potentially suspicious behavior. This includes analysis of behavioral patterns, transactional behavior, client profiles, and the nature of the services used. In the context of anti-money laundering obligations, CDD involves several stages such as identifying the potential client, verifying their identity and age, gathering supplementary information to build an economic profile, assigning a risk score, and observing the client's behavior over time for any anomalies that may suggest violations of anti-financial crime legislation.

To support this process, NUMERETO B.V. uses publicly accessible resources for background checks, including reviews of social media activity, property ownership status, employment verification, insolvency checks, and similar investigations. When the initial client review indicates low risk, simplified due diligence may be considered. However, enhanced due diligence (EDD) is mandatory when the system detects higher-risk factors, such as connections to politically exposed persons (PEPs) or residence in high-risk countries.

The Company maintains a risk scoring model that classifies clients based on key risk indicators such as geographic location, transaction history, and the specific products they engage with. The security and integrity of NUMERETO B.V.'s gaming platform is safeguarded through a blend of modern technologies and external compliance tools. This includes proprietary anti-fraud software used during onboarding and throughout the customer lifecycle, artificial intelligence (AI) mechanisms, biometric identification where applicable, and regulatory technology (RegTech) platforms such as WorldCheck, LexisNexis, etc..

NUMERETO B.V. is committed to upholding regulatory standards that explicitly prohibit the use of anonymous or fictitious player accounts. To mitigate risks related

to money laundering, terrorism financing, or the financing of weapons proliferation, player identities must be verified, and the nature of the business relationship clearly understood. A comprehensive CDD framework ensures that all regulatory obligations are met. Suspicious activity identified through monitoring or alerts will be reported to the Financial Intelligence Unit (FIU), and in relevant cases, to the public prosecutor.

The Client Acceptance Policy (CAP) in place classifies players as low, medium, or high risk, based on numerous factors such as country of residence, financial behavior, and source of income. The CAP also outlines scenarios in which services will be denied due to unacceptable levels of risk. More details on these criteria are outlined in Appendix IV.

7.1 Application of Client Due Diligence Measures

CDD is implemented under the following conditions:

- When a single transaction equals or exceeds the amount of NAF 4,000
- When occasional transactions surpass the same threshold
- When there is a suspicion of involvement in illicit financial activity
- When previously collected identity data is found to be questionable or insufficient
- When multiple smaller transactions are linked and together exceed the NAF 4,000 threshold

In high-risk cases, enhanced due diligence is mandatory.

As part of its CDD procedures, the Company will:

- Conduct identity verification using independent, credible documentation or digital sources. This includes identifying and confirming the beneficial owners of legal entities and understanding how control is exercised within such structures.
- Perform ongoing due diligence by monitoring client transactions for consistency with known risk profiles and, where appropriate, verifying the source of funds.
- Enforce confidentiality procedures ensuring that employees do not reveal the existence of any reports made to the FIU. If suspicions arise, the reporting process takes precedence over the standard CDD timeline.

7.2 Identity Verification and Information Collection

To confirm a player's identity, the following data will be collected:

- Full legal name
- Residential address

- Date and place of birth
- Nationality
- Identification number

For lower-risk cases, only the basic required data is collected. For higher-risk clients, a broader set of information is required to appropriately mitigate potential ML/TF risks. Players will initially be assigned a risk level based on the available information, which will be refined as the client relationship develops and new data is collected.

Identity verification methods include:

- Reviewing official documents such as passports or national ID cards
- Supporting proof of address via recent utility bills or bank statements, dated within the past six months
- Confirming residential addresses through direct communication (e.g., email, telephone, or mail)
- Supplementary verification methods including biometric authentication, analysis of funding methods, and IP address tracing

If initial documentation is incomplete or raises concerns, further steps such as a video selfie with identification or verifying the first deposit with a regulated payment provider may be undertaken.

The Company also seeks to understand the purpose and expected nature of the client relationship. When this is not self-evident, additional information will be collected. For higher-risk clients, comprehensive data regarding their source of wealth and expected transaction volume is required. For lower and medium-risk clients, information such as employment status or type of business is sufficient, though additional verification may be performed where necessary.

7.3 Timing of CDD Measures

NUMERETO B.V. ensures that client identification procedures are executed at the earliest stage of the relationship and in full compliance with AML/CTF/CPF laws.

Application Based on Transaction Volume

During account creation, clients must submit their name, address, and date of birth, which is then verified. All players are screened against PEP and international sanctions databases. Any transaction, whether single or cumulative, that meets or exceeds NAF 4,000 triggers full identity verification. This includes multiple smaller transactions that together reach the threshold within a relevant timeframe.

Proactive Implementation

In most cases, CDD is conducted at the point of registration, regardless of whether a transaction threshold is met, to ensure risks are mitigated early.

Interim Restrictions

If a client reaches the NAF 4,000 threshold without completing verification, the Company applies interim measures:

- For deposit-triggered thresholds, further deposits or withdrawals are blocked while gameplay with existing funds is permitted.
- For withdrawal-triggered thresholds, the account is temporarily suspended pending verification.

Escalation for Non-Compliance

Clients who fail to complete CDD within 30 days are subject to the following actions:

- If suspicious activity is detected, a Suspicious Transaction Report (STR) is filed with the FIU
- If no suspicion arises, remaining balances are refunded to the originating financial account
- If risks remain unresolved, the Company may freeze the funds as per internal protocols

Avoiding Tipping Off

In all actions, the Company exercises discretion to prevent any behavior that may constitute tipping off the client about regulatory procedures. Staff are trained to follow strict internal protocols to uphold confidentiality and compliance.

Ongoing Monitoring

CDD procedures are applied throughout the entire client relationship, not just during onboarding. NUMERETO B.V. actively monitors client behavior, conducts periodic reviews, and reassesses risk ratings based on evolving client profiles.

Risk-Based Reviews

Clients are reviewed periodically based on their assigned risk levels. If their behavior changes, or external regulatory updates occur, the company reassesses the risk classification and applies new due diligence requirements accordingly.

Trigger-Based CDD Reapplication

Full due diligence is re-applied in specific cases such as:

- Significant changes in client activity or profile (e.g., large deposits, relocation, or becoming a PEP)
- Changes to regulatory frameworks requiring stricter verification
- Reaching cumulative transaction thresholds again (NAF 4,000 or more)

Historical Gaps Remediation

For legacy accounts that were onboarded prior to current regulatory procedures, the Company undertakes retrospective due diligence. High-risk clients are prioritized, while others are reviewed on a risk basis.

These reviews include verifying the identity, performing sanctions and PEP screenings, and rechecking the sources of wealth and funds. CDD is always applied proportionately to the level of risk, ensuring efficiency while maintaining regulatory integrity.

Termination of Relationships

NUMERETO B.V. reserves the right to terminate business relationships where the client fails to meet CDD obligations or is found to pose unacceptable risks. This includes cases involving suspicious activity, non-submission of required documentation, or connection to financial crime or sanctions.

Prior to closure, the Compliance Officer conducts a full review of the client's activity. If suspicion of ML/TF/PF exists, a Suspicious Transaction Report is submitted immediately. All client records are stored for at least five years post-termination, as required by law.

If the risk cannot be mitigated or if the client is uncooperative, the relationship is terminated and the case reported to the FIU where appropriate.

Third-Party Reliance

In certain controlled situations, NUMERETO B.V. may rely on qualified third parties to assist with elements of the CDD process. However, this reliance does not diminish the Company's legal responsibility. NUMERETO B.V. remains fully accountable for the accuracy, completeness, and timeliness of all due diligence tasks.

The Company ensures that any third-party provider is supervised under AML/CTF regulations and contractually bound to share verification data promptly. Third-party arrangements are documented clearly, including data sharing procedures and the provider's obligation to comply with audits.

It is critical to distinguish between *third-party reliance* and *outsourcing*. The former allows the third party to perform duties independently, whereas outsourcing means

the third party works directly under NUMERETO B.V.'s policies and compliance framework.

Before engaging a provider, the Company conducts a detailed jurisdictional risk analysis, checking the regulatory history of the provider and ongoing performance through periodic evaluations. Risk classification and decision-making remain under the sole authority of NUMERETO B.V., ensuring continued compliance.

7.4 Beneficial Ownership and Control Structure Verification

NUMERETO B.V. applies all reasonable efforts to identify and verify the ultimate beneficial owners (UBOs) of legal entity clients. This includes both direct and indirect ownership, as well as understanding the mechanisms through which control is exercised.

Verification measures include:

- Identifying natural persons owning or controlling at least 25 percent of the entity, whether directly or indirectly
- Where no such person is identified, determining who exercises control through voting rights, board representation, or other contractual arrangements
- Conducting analysis of complex corporate structures involving trusts, nominee holders, or layered ownership
- Reviewing documentation such as shareholder lists, company formation documents, declarations, and organizational charts
- As a last resort, identifying the most senior managing official as the UBO in accordance with international standards

All ownership data must be verified using reliable and independent sources, recorded securely, and updated as required by law or when relevant changes occur. The Company does not maintain relationships with entities that are intentionally opaque or obstructive during due diligence.

8. TRANSACTION MONITORING

Transaction monitoring within the betting and gaming sector is a cornerstone of compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) frameworks. Due to the inherently high volume and rapid pace of financial activities in this industry, the risk of these platforms being exploited for illicit purposes such as money laundering, terrorist financing, or fraud is significant. Recognizing this, Numereto B.V. has designed a robust monitoring program to detect, evaluate, and

respond to suspicious activity in real time, particularly where the use of digital payment methods and cryptocurrencies creates additional complexity.

The regulatory framework in Curaçao emphasizes the importance of recognizing indicators of unusual transactions, as outlined by the Ministerial Decree and enforced by the Financial Intelligence Unit of Curaçao (FIU Curaçao). As part of its licensing obligations, Numereto B.V. ensures that its transaction monitoring system is capable of detecting such indicators and triggering appropriate internal and external reporting mechanisms.

The company's anti-fraud function is responsible for operating a proprietary monitoring infrastructure that processes large volumes of player data on a continual basis. This infrastructure consists of both automated controls and human oversight. Automated controls include real-time surveillance mechanisms configured to detect predefined patterns, thresholds, and anomalies. These systems are integrated with external databases such as WorldCheck and other AML/CTF platforms. In parallel, a dedicated team of fraud analysts performs manual investigations, utilizing various independent data sources to validate alerts and ensure that findings are reliable and substantiated.

When an initial discrepancy or red flag is identified by the first line of defense, it is escalated to the team lead for further analysis. If the anomaly meets internal criteria for suspicion, an internal Suspicious Activity Report (SAR) is submitted to the company's designated AML/CTF Officer. This Officer is then responsible for reviewing the case, determining if external reporting obligations are triggered, and submitting a report to the FIU Curaçao where necessary.

The automated transaction monitoring system employed by Numereto B.V. is specifically designed to process transactions in real time, applying rule-based logic and machine learning algorithms to detect risk indicators. These include large-value deposits or withdrawals, rapid-fire bets or gameplay patterns, frequent player-to-player transfers, or transactions involving high-risk jurisdictions. The system adapts dynamically to changing typologies and threats, improving detection while minimizing false positives.

The parameters programmed into the system are regularly reviewed and updated to ensure that they reflect both current and emerging financial crime risks. Risk scenarios that warrant heightened scrutiny include, but are not limited to:

- Sudden spikes in transaction volume or velocity
- Irregular cross-border transfers involving high-risk or sanctioned jurisdictions
- The use of multiple funding sources or mismatched account holder information
- Frequent use of anonymous or semi-anonymous payment methods

- Attempts to circumvent account verification requirements through structured transactions

In addition to reactive monitoring, the system is also capable of predictive analytics, using historical data to flag potentially suspicious future activity based on established patterns. This proactive approach allows the company to take preventative measures before suspicious activity fully materializes.

Transaction monitoring results are retained in accordance with applicable legal requirements. All flagged transactions, internal escalation records, SARs, system logs, and final determinations are securely documented and stored for a minimum period of five years. These records are maintained in a manner that ensures integrity, retrievability, and availability to competent authorities during inspections or audits.

By maintaining a highly responsive, technology-supported transaction monitoring framework and integrating it with its wider compliance and risk management systems, Numereto B.V. reinforces its commitment to detecting and preventing financial crime. The company continuously reviews and refines its controls to stay aligned with evolving regulatory expectations and global best practices in AML/CTF/CPF compliance.

Components of Numereto B.V.'s Transaction Monitoring Program

Automated Monitoring: Real-time monitoring is performed through advanced software solutions capable of recognising patterns and deviations that could indicate money laundering or other financial crime risks. Machine learning models are trained to distinguish between standard behaviour and anomalies.

Risk-Based Assessment: Clients and their transactions are evaluated using a multi-factor risk scoring system. Risk indicators include frequency and size of transactions, client location, historical behaviour, and product usage.

Alerts and Review: Whenever an alert is generated, it is assessed manually by the Compliance Officer to determine whether further investigation or escalation is warranted. Alert criteria include unusually large transactions, frequent deposits or withdrawals, and behavioural inconsistencies.

Monitoring Techniques: Risk identification tools include geolocation checks, verification of source of funds for large transactions, and behavioural analytics that assess changes in gambling patterns, frequency, and speed of financial movement.

Circumstances Triggering CDD Measures

Client Due Diligence (CDD) is initiated in several scenarios. These include account registration, inconsistencies in submitted information, unusual behavioural or

transactional patterns, and unauthorised changes to a client's profile. Additionally, when a single transaction or a group of transactions that appear linked equals or exceeds 4,000 Netherlands Antillean Guilders (NAF), CDD is applied. Such transactions include deposits, wagers, or withdrawals, whether executed separately or as part of a series. Periodic file reviews and continuous transactional monitoring also serve as triggers for reassessment.

Use of IP and Behavioural Tracking

To further support fraud detection and AML efforts, Numereto B.V. uses tools embedded within its proprietary anti-fraud system to monitor IP addresses. This helps verify that clients are not accessing services from prohibited jurisdictions and detects efforts to create multiple accounts or bypass restrictions, including those for self-excluded users. The software continuously collects and analyses data on user history, betting amounts, win/loss trends, session durations, geolocation, and behavioural patterns.

Where the client's profile is considered high risk, either due to behaviour or transaction history, the system intensifies its scrutiny. Triggers may include attempts to avoid detection, unusually structured transactions, or a combination of risk indicators.

Inability to Complete CDD and Account Closure

If CDD procedures cannot be completed due to the client's refusal to provide documentation or other verification failures, the client account is suspended pending resolution. If the verification cannot be completed within a reasonable period, the business relationship is terminated.

When accounts are closed under these circumstances, and there is no reasonable suspicion of criminal activity, the remaining funds are refunded to the original payment method. However, if suspicions persist, the company follows its escalation process to determine whether to freeze the funds and submit a report to the FIU. In every instance, the action taken is fully compliant with applicable AML and CFT requirements.

9. POLITICALLY EXPOSED PERSONS (PEP's)

Enhanced Due Diligence (EDD) is a vital part of the compliance process within the online betting and gambling sectors. It plays a central role in preventing money laundering, fraud, and related financial crimes. EDD refers to the additional verification steps applied to clients who are identified as posing a higher level of risk,

based on their profile or behavior. Among these, Politically Exposed Persons (PEPs) represent a category requiring the highest level of scrutiny.

PEPs are individuals who currently hold, or have recently held, prominent public roles. This includes, but is not limited to, heads of state, members of parliament, senior government officials, ambassadors, military leaders, directors or board members of state-owned enterprises, and individuals who hold leadership positions within international organizations. The definition of a PEP is extended to include their immediate family members and close associates, as these relationships may increase the risk of corruption or misuse of influence.

At Numereto B.V., all clients identified as PEPs, including their relatives and known associates, are automatically categorized as high-risk. Once identified, their onboarding and ongoing management is handled with heightened caution and oversight.

The Compliance Officer and senior management of Numereto B.V. oversee the evaluation and approval process for all clients designated as PEPs. No business relationship with a PEP may be initiated or maintained without prior documented approval from senior-level management. This ensures a proper chain of accountability and risk control in high-risk relationships.

Additionally, the Compliance Department maintains a secure internal register of all identified PEPs. This log includes information on the nature of the client's political exposure, relevant associations, and the justification for the risk classification. The register is updated continuously and forms part of the company's internal compliance records, readily accessible for audit and regulatory review.

Screening for PEP status is conducted at the time of onboarding and continues throughout the business relationship. Numereto B.V. uses advanced screening solutions, including risk intelligence tools such as WorldCheck and LexisNexis, to detect clients who fall into the PEP category. Regular re-screening is performed to account for changes in status or new information that may alter a client's classification.

When dealing with PEPs, additional due diligence measures are implemented, including but not limited to:

- Verifying the source of funds and wealth to ensure transparency and legitimacy
- Conducting comprehensive background checks, including adverse media reviews
- Requiring sign-off from senior management for onboarding and ongoing activities
- Increasing the frequency and depth of transaction monitoring

- Applying restrictions on high-risk jurisdictions linked to the PEP or their activities

All interactions with PEPs are closely monitored for unusual behavior, transaction patterns, or attempts to obscure financial trails. The company ensures that any suspicious activity related to a PEP is reported immediately to the Financial Intelligence Unit (FIU), in accordance with applicable AML/CFT/CPF reporting obligations.

Through these enhanced measures, Numereto B.V. ensures that it does not become a vehicle for laundering the proceeds of corruption or facilitating financial misconduct tied to politically influential individuals. The company's approach aligns with the Curaçao Gaming Control Board (GCB) regulations and international standards established by the Financial Action Task Force (FATF).

10. SANCTIONS MANAGEMENT, FATF, HIGH-RISK & LICENSE RESTRICTIONS

Sanctions screening plays a central role in preventing illegal financial activities and maintaining compliance with international laws and standards. It involves checking individuals, entities, and transactions against official sanctions lists to ensure that no engagement is made with prohibited parties. This practice helps prevent money laundering, terrorist financing, proliferation financing, and other criminal acts. For Numereto B.V., sanctions screening is not only a legal requirement but also a fundamental part of preserving the integrity and reputation of the company within the online betting and gambling industry. For a detailed Sanctions Policy, please refer to **Appendix II (Sanctions Policy)**.

While Enhanced Due Diligence (EDD) is used to manage higher-risk clients through deeper identity and activity checks, sanctions screening specifically focuses on detecting and preventing any dealings with parties listed on national, regional, or international sanctions registers.

As a company based in Curaçao with an EU-based payment partner, Numereto B.V. aligns its operations with the leading international sanctions frameworks. The following sanctions lists are monitored and applied rigorously within the company's screening program:

- United Nations Security Council (UNSC) Sanctions
<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

- European Union (EU) Sanctions
https://www.eeas.europa.eu/eeas/european-union-sanctions_en
- United States Sanctions (OFAC – Office of Foreign Assets Control)
<https://sanctionssearch.ofac.treas.gov>
- United Kingdom Sanctions (HM Treasury)
<https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>
- Other relevant national or local sanctions applicable under the jurisdictions in which Numereto B.V. operates.

In any instance where a match is identified between a client or transaction and a party listed on a sanctions register, Numereto B.V. will act immediately to freeze all associated assets. This is done without prior notification to the client and in strict accordance with the Freezing of Resources Protocol as issued in the National Gazette (2016). The company promptly notifies the Financial Intelligence Unit (FIU) of Curaçao and takes all necessary steps to ensure legal compliance.

Sanctions screening software used by Numereto B.V. is designed to synchronize automatically with official list publications. These systems ensure that any updates to sanctions registers are reflected in real-time, thereby maintaining the integrity and accuracy of the screening process. In addition to this, the Compliance Officer is responsible for conducting a monthly manual review of any regulatory circulars, updates, or changes issued by the Curaçao Gaming Control Board or other competent authorities to confirm that the internal systems remain current and aligned with local obligations.

Update Mechanism and Frequency

Sanctions lists used by the company are updated at least once per day and also immediately whenever new sanctions are published by the competent regulatory or government bodies. The automated tools used by Numereto B.V. are configured to synchronize directly with official databases to reflect updates without delay.

In addition to automated updates, the Compliance Officer or designated Sanctions Officer performs regular manual checks. At a minimum, a monthly review is conducted to cross-check any amendments or guidance published by the Curaçao Gaming Control Board or similar authorities. This ensures the company does not rely solely on automation but incorporates manual oversight to reinforce accountability and compliance accuracy.

Roles and Responsibilities

The responsibility for sanctions screening lies primarily with the Compliance Officer or a designated Sanctions Officer if appointed. This individual is tasked with ensuring that the screening tools are updated and functioning as intended, verifying the integration of updates, and reviewing all alerts and possible matches generated by the system. Confirmed matches must be escalated immediately for further investigation and reporting in accordance with the applicable laws.

The Compliance Officer must also ensure that all internal staff are trained on sanctions compliance and understand the implications of false positives, missed alerts, and failure to escalate confirmed matches. Furthermore, the officer must verify that all alerts, investigations, updates, and resolution steps are accurately documented.

All records relating to sanctions screening — including update logs, alerts, actions taken, and final match resolutions — are securely retained in line with legal and regulatory requirements. Numereto B.V. maintains these records for a minimum of five years. They are stored in a secure and retrievable manner and are made readily available to regulatory authorities during inspections, audits, or upon official request.

By maintaining a strong and dynamic sanctions management process, Numereto B.V. strengthens its ability to detect and prevent financial crimes, ensures adherence to national and international regulations, and upholds its reputation as a compliant and responsible actor in the iGaming industry. The company's detailed treatment of sanctions can be accessed through **Appendix II (Sanctions Policy)**.

11. SUSPICIOUS ACTIVITY & TRANSACTION REPORTING

For NUMERETO B.V., reporting suspicious activities within the betting and gaming industry is a fundamental obligation under both local and international financial crime prevention regulations. These reports play a central role in protecting the integrity of the platform and preventing its misuse for unlawful purposes such as money laundering (ML), terrorist financing (TF), fraud, or corruption.

Timely and accurate reporting serves several critical functions. Beyond fulfilling legal obligations, it helps protect clients from exploitation, fosters trust in the gaming environment, and shields the business from reputational and regulatory risks. Any failure to report a suspicious activity, whether intentional or due to negligence, may lead to serious legal penalties, including fines and criminal sanctions.

Suspicious activities may manifest through various forms of transactional or behavioral anomalies. These include, for example, structured deposits or withdrawals, sudden changes in account usage, disproportionately high wagers, or

indifference to gambling outcomes. Such indicators may be signs of financial crime or merely atypical behavior requiring further review.

NUMERETO B.V. takes a two-tiered approach: First, unusual behavior is flagged and reviewed to determine if it is merely irregular or raises suspicion of a connection to criminal proceeds. If suspicion is confirmed, a formal internal report is submitted to the nominated AML/CFT Officer, who evaluates whether the matter must be escalated to the Financial Intelligence Unit (FIU) of Curaçao.

Pursuant to Article 1 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), entities conducting internet gambling activities are required to submit reports of unusual transactions through the FIU Curaçao's official reporting platform: the goAML portal, which has been in mandatory use since 1 January 2021. If a case qualifies for external reporting, the nominated officer must file it via the portal in accordance with internal AML/CTF policies.

While a decision is pending or after a report is made, the business relationship with the involved client must be temporarily suspended or, if warranted, permanently discontinued based on the severity of the concern.

Internal Reporting Obligations

All staff at NUMERETO B.V. are required to raise a report internally if they have knowledge, suspicion, or reasonable belief that a client is attempting to launder money or finance terrorism. Upon such internal notification, the AML officer must determine whether the facts meet the threshold for filing a Suspicious Activity Report (SAR) with the FIU.

11.1. Examples of Suspicious Activity

Suspicious behavior may include a combination of transactional and profile-related indicators, such as:

- Repeated use of anonymous payment channels (e.g., prepaid cards or gift cards).
- Inconsistency between geolocation data and the origin of payments.
- High-value deposits followed by immediate withdrawals with little or no gambling activity.
- Withdrawals routed to third-party payment methods.
- Refusal to cooperate with identity verification or unusual reliance on intermediaries.
- Source of wealth inconsistent with the client's declared financial position.
- Rapid or frequent changes in account ownership.
- Hesitancy or outright refusal to submit required due diligence documents.

All such activity is recorded meticulously, including transaction dates, methods, monetary amounts, and other relevant attributes. The compliance and anti-fraud teams also compile comprehensive client data such as names, addresses, ID numbers, and account history for internal analysis and possible disclosure.

11.2. Identifying Unusual Transactions

An unusual transaction is any financial activity that significantly diverges from a client's normal or expected pattern of behavior, especially if it lacks a clear legal or economic rationale. NUMERETO B.V. considers the following as examples:

- Sudden large deposits or withdrawals without clear justification.
- Transactions involving third parties not previously associated with the account.
- Financial movements inconsistent with the customer's known profile or declared income.

The company's automated transaction monitoring system continuously scans for such anomalies. Alerts generated by this system are promptly forwarded to the Compliance Officer for further assessment. Staff are trained to recognize both behavioral and transactional red flags and to escalate concerns immediately through proper channels.

Categories of Noteworthy Transactions

Several categories of transactions require closer scrutiny:

- **Previously Flagged Transactions:** Activities already reported to law enforcement or judicial bodies for suspected links to ML or TF are automatically deemed unusual.
- **Dealings with Sanctioned Parties:** Any interaction involving individuals or entities listed under the Sanctions National Ordinance (N.G. 2014 no. 55) or other applicable sanction regimes is flagged for reporting.
- **High-Value Transactions:** All single transactions valued at or above 5,000 Netherlands Antillean Guilders (NAF), whether via deposit, withdrawal, or purchase of digital tokens, require further examination. This also applies to multiple linked transactions on the same day that cumulatively exceed the NAF 5,000 threshold.

In any instance where there is a reasonable suspicion that a transaction is linked to money laundering, terrorism financing, or proliferation financing—whether due to the transaction's structure, the client's behavior, or contextual risk indicators—it must be escalated internally without delay.

11.3. Timely Submission of Reports to FIU

Once a transaction has been deemed unusual or suspicious, NUMERETO B.V. must file a report with the FIU Curaçao without delay, as outlined in AML Regulation IV.1. This obligation applies even if the transaction is incomplete or only attempted.

The Unusual Transaction Report (UTR) is submitted by the Compliance Officer immediately upon confirming suspicion, with no requirement for additional approval steps or internal sign-off processes. Timeliness is paramount, and delays in reporting could result in regulatory non-compliance.

11.4. Confidentiality of Suspicious Activity Reporting

The confidentiality of the SAR and UTR processes is critical. All employees are strictly prohibited from disclosing information relating to the submission or consideration of a suspicious activity report. This includes revealing the existence of the report to the subject of the investigation or to any unauthorized party.

Such disclosures may constitute a “tipping-off” offence under Curaçao law and undermine the integrity of ongoing investigations. Only the Compliance Officer and other authorized compliance personnel may access SAR-related information.

To uphold this confidentiality standard, NUMERETO B.V. provides ongoing staff training focused on the sensitivity of suspicious transaction reporting. Any breach of these protocols is treated as a serious compliance violation and may result in disciplinary measures, including termination of employment.

11.5. Commitment to a Strong Reporting Culture

By fostering a corporate culture centered on vigilance, confidentiality, and regulatory accountability, NUMERETO B.V. enhances its capacity to identify suspicious conduct, uphold its AML/CTF/CPF responsibilities, and contribute effectively to the global fight against financial crime in the iGaming sector.

12. COMPLIANCE OFFICER

The Compliance Officer, also referred to as the Money Laundering Reporting Officer (MLRO), is the appointed person responsible for overseeing the Anti-Money Laundering (AML) compliance framework within NUMERETO B.V. This role is critical to ensuring full alignment with legal obligations, regulatory expectations, and internal risk controls. The Compliance Officer is authorised to engage directly with competent authorities in Curaçao and holds overall responsibility for managing the day-to-day functions of the AML team. These responsibilities include enforcing effective age verification measures, advancing responsible gambling policies, supporting player self-exclusion mechanisms, and monitoring for gambling-related harm.

Within NUMERETO B.V., the Compliance Officer operates independently from the commercial and operational units of the company. This independence ensures that compliance-related decision-making remains impartial and free from conflicts of interest. The Compliance Officer reports directly to the Board of Directors and is granted full access to all customer records, transaction history, internal systems, and staff whenever such access is required to carry out compliance duties efficiently.

The Board is responsible for ensuring that the Compliance Officer has sufficient authority, resources, and operational capacity to implement the Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CTF/CPF) program effectively. This governance model is aligned with Regulation V.3 of the AML Guidelines issued by the Curaçao Gaming Authority and enables direct escalation of critical matters to the highest level of corporate oversight.

In line with legal obligations and the company's reporting protocols, the Compliance Officer is also responsible for preparing and submitting Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs) to the Financial Intelligence Unit (FIU) of Curaçao when a suspicious transaction or activity is detected. Internally, the Compliance Officer must compile and present quarterly AML reports to the Board of Directors. These reports provide updates on AML/CTF compliance performance and may include recommendations for improving the control environment or enhancing specific aspects of the company's risk management strategy.

The duties of the Compliance Officer encompass the following core areas of responsibility:

- **Policy Implementation:** Leading the rollout and operational integration of AML policies and procedures to ensure consistency with national laws and international expectations.

- **Central Point of Contact:** Acting as the principal liaison for all AML-related inquiries, issues, or escalations, both internally and externally.
- **Policy Maintenance and Review:** Conducting periodic evaluations of the company's AML policies, making necessary amendments to address emerging risks, legal updates, or procedural inefficiencies.
- **Training and Awareness:** Designing and overseeing the AML training framework to ensure that all relevant employees are knowledgeable about their responsibilities in identifying, escalating, and reporting suspicious activity.
- **Transaction Monitoring and SAR Submission:** Carrying out regular reviews of customer transactions and behaviour to identify red flags indicative of potential money laundering or terrorism financing. Where suspicious activity is confirmed, the Compliance Officer prepares and submits SARs to the FIU in accordance with regulatory timelines.
- **Policy and Framework Development:** Establishing and updating the company's AML policies in response to changes in the legal environment, risk landscape, or industry standards, with a focus on practical implementation and enforcement.
- **Employee Training Management:** Ensuring staff training programs are both mandatory and ongoing. This includes the development of materials that reflect current laws, regulatory guidance, and internal policy updates.
- **Regulatory Liaison:** Engaging with supervisory authorities, law enforcement, and other competent bodies on behalf of NUMERETO B.V. in relation to AML/CTF inquiries, data requests, or compliance inspections.
- **Audit and Self-Assessment:** Performing internal audits to assess the design and operational effectiveness of the AML framework. Any deficiencies identified during these audits are remediated through corrective actions that are tracked and reviewed for effectiveness.
- **Record Maintenance:** Keeping complete and secure records of AML activities. This includes maintaining registers of SARs, internal alerts, training logs, policy changes, and internal communications related to AML oversight. All records are stored in accordance with data protection standards and are made available for audit or regulatory review upon request.

Through the execution of these duties, the Compliance Officer at NUMERETO B.V. plays a central role in protecting the company from being exploited for illicit purposes and ensuring continued compliance with Curaçao's AML legislative and regulatory regime.

13. SENIOR MANAGEMENT RESPONSIBILITIES

At NUMERETO B.V., senior management maintains a central and active role in overseeing the assessment and management of inherent AML/CTF/CPF risk categories. The Board of Directors requires the appointed AML/CFT Officer to regularly provide updates on any significant issues or deviations observed in the company's control environment. Additionally, the officer must prepare a comprehensive annual report evaluating the adequacy of internal systems and procedures in place to mitigate the risks associated with money laundering, terrorist financing, and the financing of weapons proliferation.

The company's policies and procedures are reviewed on a quarterly basis, with guidance provided by the outcomes of monthly risk assessments. Where potential weaknesses in internal controls or risk management practices are identified, the AML/CFT Officer may submit formal proposals for policy amendments to the Board of Directors. Such proposals are evaluated and approved as needed to ensure that the company's risk controls remain effective and compliant with evolving regulatory requirements.

Policy Review and Risk Assessment

Senior management holds full accountability for reviewing all relevant AML, CTF, and CPF policies at least once every year. These annual reviews are informed by continuous monthly risk assessments, which serve to highlight any new or emerging vulnerabilities within the operational or compliance framework. If deficiencies or gaps are found, the AML/CFT/CPF Officer is responsible for recommending corrective actions to the Board, ensuring that timely and strategic enhancements are implemented across the company's systems and procedures.

Employee Training Programs

In accordance with international regulatory standards and industry best practices, senior management is tasked with overseeing the development and implementation of robust employee training programs. These training initiatives are designed to ensure that staff across all departments, particularly those in key compliance and risk-related roles, are equipped with the knowledge and tools necessary to identify and respond to suspicious activity. This includes raising awareness of the signs of money laundering, understanding the procedures for reporting concerns, and maintaining compliance with the company's risk-based approach.

Internal Control Framework

The leadership of NUMERETO B.V. is also responsible for maintaining a strong and clearly defined internal control structure. This structure ensures the implementation of effective safeguards, including the separation of duties, proper authorization

procedures, regular oversight mechanisms, and comprehensive record-keeping practices. Senior management ensures that compliance measures are not only adopted but enforced throughout the organization.

To ensure independent oversight and continued improvement of the AML/CTF/CPF program, senior management commissions regular audits and independent assessments. These evaluations provide objective feedback on the performance of the company's compliance systems and help to identify areas for improvement or reform. Findings from these audits are used to strengthen operational resilience, close any gaps in controls, and uphold the company's obligations under Curaçao's regulatory framework.

14. EMPLOYEE TRAINING AND SCREENING PROGRAMME

Personnel working in the gaming and betting sector represent a crucial line of defense in the fight against money laundering and terrorist financing. Numereto B.V. operates with a strong ethical foundation, ensuring adherence to applicable laws and regulations governing financial activities. To uphold its standards of integrity, the company has put in place robust employee screening procedures, including checks for criminal records and other risk factors.

In accordance with Regulation V.4 of the CGA AML Guidelines, Numereto B.V. maintains a structured **Employee Screening and Monitoring Program (Appendix IV)** to evaluate the integrity and competence of all individuals involved in roles tied to AML and CTF responsibilities. For further reference, see Appendix II.

Employees are made fully aware that failure to identify or escalate potential violations of AML/CFT obligations may lead to regulatory sanctions and, where applicable, criminal prosecution.

AML/CFT Role Awareness

All employees, particularly those handling customer interaction or financial processes, are expected to possess a comprehensive understanding of the company's AML/CFT/CPF policies. This includes the ability to identify indicators of suspicious behaviour, follow appropriate internal reporting channels, and protect the confidentiality of customer information throughout the process.

Staff must remain alert to unusual or irregular activities that deviate from normal user conduct—such as inconsistent or excessively large bets, unexplained shifts in betting patterns, or financial movements lacking an economic purpose.

Once a concern is identified, the employee must report the matter promptly to the Compliance Officer through the established internal reporting mechanisms. This includes filing a Suspicious Activity Report (SAR) and following the company's reporting protocols. Employees are regularly trained to ensure they understand this process and the importance of timely action.

Due Diligence by Frontline Personnel

Employees who are involved in onboarding, verification, and account management are responsible for performing initial and ongoing due diligence on customers. This includes verifying identification documents, checking the legitimacy of the declared source of funds, and screening clients against applicable sanctions or watchlists. Staff are instructed to escalate any discrepancies or concerns immediately to compliance personnel.

Additionally, employees are educated on data protection requirements and are required to uphold strict confidentiality when handling sensitive customer information, in accordance with applicable data privacy laws.

Structured Screening Program

Numereto B.V. adheres to a rigorous employee screening model consisting of **three core components**:

1. Pre-Employment Vetting

Before hiring any new team member, especially those in sensitive or high-risk roles, the company performs comprehensive background checks, including:

- Identity verification and right-to-work validation via official documentation.
- Criminal record checks to identify past offenses relevant to financial crime or ethical breaches.
- Verification of previous employment and reference checks to assess the candidate's competence and integrity.
- Screening against sanctions and Politically Exposed Person (PEP) lists using reliable databases and watchlists.

Applicants who do not meet Numereto B.V.'s integrity and risk standards are not permitted to proceed with employment.

2. Ongoing Screening and Monitoring

Employee vetting does not end upon hire. The company carries out continual assessments to ensure personnel remain fit and proper for their roles:

- **Annual re-screening** for staff in compliance-sensitive or high-risk positions.
- **Event-based screening**, triggered by incidents such as suspected misconduct, changes in responsibilities, or role transitions.
- Ongoing monitoring of any changes in legal status, PEP classification, or exposure to sanctions.

All results are retained securely and in compliance with data protection regulations, for a minimum of five years.

3. AML Training and Capacity Building

Numereto B.V. conducts **mandatory AML/CTF/CPF training** at least once annually for employees involved in onboarding, transaction processing, or customer relationship management. This training ensures staff understand:

- Their specific responsibilities under the AML/CTF/CPF program.
- How to identify red flags, including:
 - Large or inconsistent betting behaviour.
 - Unusual deposit and withdrawal activity.
 - The use of anonymous, unverified, or third-party payment instruments.
- The correct procedure for reporting suspicious behaviour, including completing and submitting SARs.
- The importance of safeguarding client confidentiality and adhering to data protection laws.

Failure to follow AML protocols or to report suspicious activity may lead to internal disciplinary measures and, in some cases, external legal or regulatory consequences.

15. RECORD-KEEPING

Numereto B.V. complies with all applicable laws and regulatory requirements concerning the maintenance of an audit trail, especially in scenarios where cooperation with law enforcement authorities is necessary for investigative purposes. All records created in this context are retained in digital format for a minimum of five years. This retention period begins from the date on which a business, commercial, or professional relationship is initiated with an employee, client, or business partner, in line with applicable data protection and AML regulations.

In order to meet rigorous record-keeping standards, the company has implemented structured procedures designed to manage all documentation connected with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance. The company maintains a comprehensive archive of documents which includes, but is not limited to, client identification data, transactional records, internal suspicious activity reports, employee training documentation, and audit logs. All these records are securely preserved for no less than five years, unless longer retention is required by law or regulatory guidance.

The company ensures the secure storage of this data through the use of advanced encryption methods and strict internal access controls. These safeguards are in place to prevent unauthorized access or tampering. In addition, periodic internal audits are conducted to verify the accuracy and integrity of the stored information and to detect any potential vulnerabilities that could compromise record confidentiality.

A structured and systematized approach is applied for indexing and organizing records. This setup enables authorized personnel and regulatory authorities to retrieve relevant documentation promptly and efficiently when needed. All data is classified according to its sensitivity and stored accordingly to meet both internal access protocols and external inspection standards.

Internal monitoring routines are conducted on an ongoing basis to review compliance with the established record management procedures. This is supplemented by regularly scheduled audits to further ensure adherence to legal obligations and internal policy frameworks.

Through diligent implementation of these record-keeping protocols, Numereto B.V. not only upholds its obligations under applicable AML, CTF, and CPF laws but also strengthens the audit readiness of the organization. Furthermore, this system contributes to the integrity and transparency of the company's gaming and financial operations and reinforces its commitment to safeguarding the regulated environment within which it operates.

16. AML COMPLIANCE AUDIT

NUMERETO B.V. acknowledges the vital role of internal auditing in maintaining the strength, transparency, and legal alignment of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance framework. Internal audits are not regarded merely as routine exercises, but rather as an essential component of the company's governance system. These audits are performed independently and diligently, producing formal findings and recommendations, which are presented directly to senior management and the Board of Directors.

In line with this commitment, NUMERETO B.V. conducts AML compliance audits on a regular basis, with such reviews taking place at least once annually, and additionally triggered whenever there are major regulatory amendments, material changes in operational workflows, or occurrences of serious compliance breaches. These audits are carried out by competent individuals or external parties with no involvement in day-to-day compliance operations, and who possess appropriate expertise in financial crime prevention and control.

The scope of each audit encompasses, but is not limited to, the following key areas:

- **Evaluation of Internal Policies and Procedures:** The audit team examines whether the current AML/CTF/CPF program is comprehensive, legally compliant, up to date with the latest regulatory requirements, and effectively implemented across all business units and operational levels.
- **Effectiveness of the Risk-Based Approach:** The auditors assess the development, application, and practical outcomes of Business Risk Assessments (BRA), Customer Risk Assessments (CRA), and any other structured risk evaluation methods used within the organization.
- **Transaction Monitoring Systems and Filing of Suspicious Activity Reports:** The audit includes a thorough review of the automated transaction monitoring processes, their coverage and sensitivity, as well as the timeliness, completeness, and accuracy of Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs).
- **Customer Due Diligence (CDD) and Know Your Customer/Business (KYC/KYB) Procedures:** A representative sample of client files is reviewed to verify whether identity verification, beneficial ownership checks, document retention, and risk classification protocols have been properly applied and documented.

- **Sanctions Screening Mechanisms:** Auditors verify that all sanctions screening tools used by the company are effectively integrated into the compliance workflow and synchronized with up-to-date international and domestic sanctions databases.
- **Employee Screening and AML Training Compliance:** The adequacy of the company's employee screening framework, both pre-employment and ongoing, is reviewed, alongside the relevance, delivery, and coverage of annual AML/CTF training programs for staff members.
- **Controls for Technology-Related Risks:** The integrity and functionality of technological systems supporting the AML program are reviewed, including user access controls, data validation mechanisms, automated risk flagging, and system audit trails.

The findings of each audit are compiled in a detailed formal report, which is submitted without delay to both the senior management and the Board of Directors. This reporting process aligns with the obligations set out in Section V.7 of the CGA AML Guidelines. These audit reports clearly outline any identified deficiencies, system gaps, or compliance risks, and propose targeted recommendations with specific timelines for remediation and follow-up.

In situations where audit results reveal significant non-compliance, control failures, or material exposure to AML/CTF/CPF risks, such issues are immediately escalated to the Compliance Officer and the Board for urgent attention. Subsequent follow-up audits or control reviews are conducted to confirm that recommended corrective actions have been implemented fully and effectively.

NUMERETO B.V. keeps an organized and secure audit trail of all internal audit activities, including documentation of findings, responses, and remedial actions taken. These records are preserved for a minimum period of five (5) years and are made readily available to the Curaçao Gaming Control Board (GCB) or other competent authorities upon request. The company remains committed to maintaining the highest standards of compliance oversight, internal accountability, and continuous improvement across all aspects of its AML/CTF/CPF control framework.

17. REGULATORY ACCESS AND COOPERATION

NUMERETO B.V. acknowledges and respects the supervisory authority and enforcement powers granted to the Curaçao Gaming Control Board (GCB), and affirms its commitment to ensuring full and proactive cooperation during all

regulatory reviews, inspections, and monitoring activities related to its AML/CTF/CPF compliance obligations.

To support the oversight mandate of the GCB and any other competent authority with jurisdiction under applicable laws, NUMERETO B.V. guarantees unrestricted, prompt, and complete access to all data, systems, records, and personnel deemed necessary for the assessment of the company's Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing framework.

This access includes—but is not limited to—the following categories of information:

- **Customer Due Diligence (CDD) files**, including enhanced due diligence where applicable.
- **Transaction histories and monitoring reports**, including flagged activities and alerts.
- **Business and customer risk assessments**, including internal risk classification methodologies and scoring outcomes.
- **AML/CTF/CPF-related policies and procedures**, along with documentation of their implementation across departments.
- **Staff communication logs**, employee certifications, and internal AML training materials.
- **Audit reports and working papers**, including records of internal and external AML audits.
- **Access to systems and platforms** used for AML transaction monitoring, sanctions screening, record-keeping, and suspicious activity reporting.

NUMERETO B.V. will facilitate on-site and remote inspections, including system walkthroughs, interviews with key personnel, document sampling, and any follow-up inquiries deemed necessary by the regulator. The company ensures that all requested information is organized, accessible, and promptly delivered, in compliance with statutory retention obligations which require such records to be maintained for no less than five (5) years, or longer where mandated by law.

In addition, NUMERETO B.V. confirms its readiness to fully engage with the post-inspection process, including the implementation of any corrective measures, enhancements to internal controls, and remedial actions issued by the GCB. All such directives are treated with priority and documented as part of the company's compliance management framework.

By upholding these standards of transparency, responsiveness, and collaboration, NUMERETO B.V. reinforces its regulatory standing and its dedication to preserving the integrity of the Curaçao gaming sector and the broader financial ecosystem.

18. INTERNAL AUDIT AND REPORTING

Numereto B.V. shall establish and uphold an independent internal audit function that serves to critically evaluate the efficiency, sufficiency, and operational soundness of the company's Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. Internal audits concerning AML compliance shall be conducted at least once per year, and may be carried out more frequently if deemed necessary due to changes in the Company's risk profile, modifications to the regulatory environment, or significant alterations in business operations.

Audits shall be performed either by a qualified in-house internal audit team or an external independent auditor, ensuring full impartiality, professionalism, and competency in reviewing AML/CTF/CPF processes. This audit mechanism is a cornerstone of the Company's broader compliance and governance strategy.

Scope of the Internal Audit

The internal audit will comprehensively address, without limitation, the following core areas:

- **Review of AML/CTF/CPF Policies and Procedures:** Verification of whether policies are up to date, compliant with legal and regulatory standards, and effectively applied across all departments and operations.
- **Assessment of the Risk-Based Approach:** Evaluation of the implementation and operationalization of Business Risk Assessments (BRA), Customer Risk Assessments (CRA), and other internal risk evaluation tools.
- **Monitoring of Transactions and Reporting of Suspicious Activities:** Analysis of the transaction monitoring system's capability to detect suspicious activities and confirmation of timely and accurate filing of Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs).
- **Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) Practices:** Examination of selected customer records to confirm the appropriate implementation of due diligence measures, beneficial ownership

checks, and proper retention of supporting documents.

- **Sanctions Screening Controls:** Review of the effectiveness, accuracy, and frequency of sanctions screening procedures against all applicable international and local lists.
- **Employee Screening and Training Programs:** Evaluation of the consistency and completeness of employee vetting processes, and assessment of the adequacy, delivery, and documentation of AML/CTF training programs.
- **Technology and Data Integrity Controls:** Scrutiny of the digital infrastructure supporting AML compliance, including system access rights, automation tools, risk scoring models, and data reliability controls.

Internal Audit Reporting

Upon completion of each audit cycle, the auditor (internal or external) shall produce a comprehensive Internal Audit Report, detailing the methodology applied, key findings, observed deficiencies, and recommended corrective measures. This report is to be submitted immediately and directly to Senior Management and the Board of Directors, or a delegated oversight committee thereof, in line with Section V.7 of the CGA AML Guidelines.

Any identified shortcomings, weaknesses, or failures in the AML/CTF/CPF control environment shall be assigned specific action items with clearly defined remediation timelines. It is the responsibility of Senior Management to ensure the implementation of these actions and to oversee full rectification in a documented and verifiable manner.

Documentation and Record Retention

Numereto B.V. shall maintain a full and secure audit trail of all AML/CTF/CPF audit activities, including but not limited to:

- Audit reports and findings
- Working papers
- Corrective action logs
- Internal approvals and follow-up documentation

All audit documentation shall be retained for a minimum of five (5) years, or for a longer duration if mandated by law or regulation. These records shall be stored in a secure, tamper-proof manner and made readily accessible to the Curaçao Gaming Control Board (GCB) or any other authorized regulatory body upon request.

Audit Access Rights

To ensure full effectiveness of the internal audit function, the appointed audit personnel shall be granted unrestricted access to all relevant systems, records, personnel, and data repositories required to fulfill their duties. There shall be no impediments—whether technical, procedural, or organizational—to the auditors' ability to conduct thorough and independent evaluations.

19. APPENDICES

Appendix I (Customer Risk Calculator)

Customer Risk Calculator														
Client no.:		NEW total score: 0.00		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Category</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>low</td> <td style="background-color: #90EE90;">0-1.8</td> </tr> <tr> <td>medium</td> <td style="background-color: #FFD700;">1.8-2.3</td> </tr> <tr> <td>high</td> <td style="background-color: #FF4500;">2.3-3.0</td> </tr> <tr> <td>unacceptable</td> <td style="background-color: #0000FF;">At least 1 photograph</td> </tr> </tbody> </table>	Category	Score	low	0-1.8	medium	1.8-2.3	high	2.3-3.0	unacceptable	At least 1 photograph
Category	Score													
low	0-1.8													
medium	1.8-2.3													
high	2.3-3.0													
unacceptable	At least 1 photograph													
Name:		NEW risk level: Low												
		Onboarding specialist:												
		Last update date:												
Risk Category	Question	Risk score	Risk level	Additional comments										
Client	Customer's Age													
Geography	Customer's Citizenship													
Geography	Customer's Second Citizenship													
Geography	Customer's Country of Birth													
Geography	Customer's Country of Residence													
Client	Does Customer have the status of PEP/RCA (Politically Exposed Person/Relative and Close Associate)?													
PROFILE														
Client	Purpose of account registration?													
SOF/SDW														
Client	Source of funds	average												
Client	Source of wealth	average												
INCOMING PAYMENTS														
Transactions	Average frequency of transactions													
Transactions	Expected total value of transactions per period (NAP)													
Transactions	Types of incoming payments	average												
OUTGOING PAYMENTS														
Transactions	Average frequency of transactions													
Transactions	Expected total value of transactions per period (NAP)													
Transactions	Types of outgoing payments	average												
Transactions	Reasons for outgoing payments	average												
BEHAVIOUR														
Products and Services	Please indicate services of interest	average												
CONFIRMATIONS														
Payment Channels	Channels	average												
Third-party involvement	Access													
Onboarding	Adverse media level													
Client														
Other	Manual risk level adjustment based on the expert judgement (0-5):			Comment regarding manual risk adjustment.										
				Summary of the applicant:										

Appendix II

Sanctions Policy

NUMERETO B.V. is obligated to adhere to legal frameworks that impose financial and other restrictions on dealings involving designated individuals, organizations, and countries. This Sanctions Policy (referred to as "the Policy") outlines the Company's internal procedures and compliance requirements that support adherence to applicable sanctions laws. Sanctions are used by national governments and international bodies as a foreign policy mechanism to deter or respond to threats against peace, security, or international law. These measures may be initiated in response to the actions of nation-states, geopolitical tensions, or transnational activities. While the scope, enforcement intensity, and regulatory requirements differ among sanctions regimes, most fall into one of the categories described below:

- **Comprehensive Sanctions:** These affect entire countries or territories (e.g., the Crimea region of Ukraine) and usually prohibit nearly all forms of engagement with the sanctioned region. The intention behind comprehensive sanctions is to impact government behavior by imposing broad economic costs, banning access to military goods or repression tools, and restricting trade and services.
- **Regime-Based Sanctions:** These target specific governments or leadership structures. Unlike comprehensive sanctions, they are generally list-based, focusing on individuals or entities associated with harmful activities such as corruption, threats to public order, or violations of democratic principles. These sanctions often come with limited trade and financial restrictions and are designed to support the rule of law and human rights.
- **Sectoral Sanctions:** These measures focus on strategic economic sectors of a country. While they do not completely restrict commercial activity, they place controls on engagements with key institutions or companies that are central to a government's political or economic power. These may affect industries like energy, defense, or finance.
- **Special Debt and/or Equity Sanctions:** This type of restriction does not prohibit general commercial engagement with listed entities but restricts their ability to raise new capital or issue new equity. These sanctions are usually applied to government-linked entities or to companies with strategic importance to a target country's economy.
- **Conduct-Based Sanctions:** These are list-based and aimed at individuals or entities involved in specific types of harmful conduct. Such conduct includes,

but is not limited to, terrorism, proliferation of weapons of mass destruction, bribery and corruption, human rights violations, drug trafficking, cybercrime, election interference, and organized crime. The purpose of these sanctions is to prevent and penalize participation in such activities.

It is important to note that the above categories may overlap in practice. For instance, an individual listed under a regime-based program may also fall under conduct-based designations if they are associated with human rights abuses or other violations.

Sanctions Regimes

Given the nature of its operations, NUMERETO B.V. falls under the jurisdiction of several international sanctions regimes, which may impact its customers, partners, products, and services. The key frameworks influencing the Company's obligations are as follows:

United Nations (UN)

The United Nations Security Council (UNSC), under Chapter VII of the UN Charter, has the authority to adopt sanctions to maintain or restore peace and international security. These sanctions are administered by UNSC sanctions committees and are supported by the Financial Action Task Force (FATF) through its Recommendations 6 and 7. All UN member states are legally required to enforce UNSC sanctions. NUMERETO B.V. complies with all UN-imposed restrictions.

European Union (EU)

Sanctions are among the tools used by the EU's Common Foreign and Security Policy (CFSP) to uphold international law, democracy, and human rights. The EU enforces all UN sanctions and may also apply its own autonomous sanctions. EU measures apply within EU territory and airspace, to EU nationals globally, to EU-registered companies including their branches outside the EU, and to activities conducted within the EU. NUMERETO B.V. ensures full compliance with these regulations across all jurisdictions where it operates.

United Kingdom (UK)

UK financial sanctions apply within the UK's territory, to all UK nationals regardless of location, to all UK-registered legal entities (including non-UK branches), and to any activity within the UK. NUMERETO B.V. complies with UK sanctions to the extent that doing so does not contradict applicable EU laws.

United States (US)

US sanctions fall into two categories:

- **Primary Sanctions:** These apply to US persons, entities incorporated in the US and their branches, as well as individuals physically located within the United States.
- **Secondary Sanctions:** These may apply to non-US persons even in the absence of a direct connection to the US, especially under programs targeting specific jurisdictions such as Iran, Russia, or Hong Kong.

NUMERETO B.V. complies with both categories to the extent allowed by applicable laws. If local or EU laws (such as Council Regulation (EC) No 2271/96) prohibit compliance with secondary sanctions, the Compliance Officer escalates the matter to the Company's Directors and Board.

Policy Statement

Under this Policy, NUMERETO B.V. commits to:

- Freeze accounts and assets of sanctioned individuals or entities where legally required.
- Refuse to engage in unlicensed financial or commercial activities involving sanctioned parties.
- Exit relationships with clients identified as sanctioned, regardless of whether local laws mandate such an action. If local laws prevent immediate termination, the matter is escalated to the Board.
- Prevent any structuring of transactions intended to circumvent sanctions laws.

Violations of this Policy may result in regulatory fines, civil or criminal penalties, and reputational harm. Employees found in breach may also face disciplinary measures including termination, and in some cases, legal consequences.

Roles and Responsibilities

Board of Directors

- Approves this Policy and ensures its communication throughout the Company.

- Oversees that the sanctions compliance function receives adequate authority and resources.
- Reviews regular compliance reports from the Compliance Officer.
- Ensures the appointment of a qualified Compliance Officer who can raise issues directly with the Board.

Directors

- Review compliance updates and escalate decisions when sanctions-related risks or conflicts of law arise.

Compliance Officer

- Conducts risk assessments for clients and transactions with potential sanctions exposure.
- Proposes updates to this Policy and ensures regulatory alignment.
- Communicates updates on sanctions developments to staff.
- Validates the completeness and accuracy of client identification documentation.

All Employees

- Maintain awareness of sanctions-related risks.
- Report suspected violations or sanctions evasion to the Compliance Officer.
- Avoid advising clients in ways that could facilitate circumvention of sanctions.
- Complete mandatory sanctions compliance training and follow internal procedures.

Sanctions Screening

NUMERETO B.V. performs sanctions screening against all clients, transactions, and third parties using an external risk management solution. This solution performs continuous screening after onboarding and compares client data against global watchlists.

Screening statuses include:

- **True Positive:** Complete match with a sanctions list.
- **Potential Match:** Partial or unclear match.
- **False Positive:** Match not associated with any actual risk or restricted activity.
- **Unknown:** Incomplete data, such as missing full name or date of birth.

Cases marked as “True Positive” or “Potential Match” are escalated to the Compliance Officer. If declined, rejection reasons such as “Sanctions”, “PEP”, “Adverse Media”, or “Criminal Records” are applied.

Sanctions sources screened include (but are not limited to):

- **European Union:** EEAS, CFSP Consolidated List
- **UK:** HM Treasury’s BOE Consolidated List, Russia-related financial restrictions
- **US:** OFAC SDN List, Entity List, Denied Persons List, Consolidated Sanctions List (OFAC-CSL)
- **UN:** UN Security Council Consolidated List

Sanctions Evasion

Sanctions regimes explicitly prohibit evasion attempts. Red flags include:

- Clients using intermediaries to disguise the involvement of sanctioned persons.
- Use of “wire stripping” to remove identifying information from transactions.
- Transactions originating from VPNs or masked IP addresses.
- Use of front companies in non-sanctioned jurisdictions.

All suspected evasion attempts are immediately reported to the Compliance Officer. Depending on the findings, they may escalate to regulators or law enforcement. Sanctions-related findings are also included in internal compliance reports.

Asset Freezing

“Asset freezing” or “blocking” refers to the restriction of sanctioned parties’ access to their assets. While ownership remains, all usage rights are restricted without regulatory approval. Assets may include cryptocurrencies and fiat balances held by NUMERETO B.V.

Sanctions Compliance Training

The Compliance Officer ensures that all employees receive:

- **Annual Training** for all staff on major sanctions regimes, obligations, and evasion techniques.
- **Risk-Based Training** for higher-risk roles, including client-facing employees and those involved in payments or compliance operations.

Training records, including attendance and materials, are retained as part of the Company’s AML framework.

Outsourcing

When sanctions-related functions are outsourced, NUMERETO B.V. retains full accountability for ensuring that outsourced services comply with this Policy and all applicable legal requirements.

Record-Keeping

All documentation related to sanctions compliance, including alerts, reviews, escalation records, and training logs, is retained in accordance with NUMERETO B.V.’s AML record-keeping policy.

APPENDIX III

Customer Acceptance Policy

NUMERETO B.V. has implemented this Customer Acceptance Policy (“CAP”) to define clear rules, responsibilities, and control mechanisms for assessing and approving prospective customers who wish to participate in its online gaming and betting services. The primary objective of this policy is to safeguard the Company against exposure to illegal activities such as money laundering, terrorist financing,

proliferation financing, fraud, sanctions evasion, and other criminal conduct, while ensuring compliance with the applicable legislative and regulatory framework in Curaçao.

This Policy is fully aligned with the guidance and regulatory expectations of the Curaçao Gaming Control Board and is an integral component of NUMERETO B.V.'s broader Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) program. It reflects international regulatory best practices, including the standards established by the Financial Action Task Force (FATF), the European Union AML Directives, and the Wolfsberg Principles.

The CAP is developed in accordance with the requirements set out under Curaçao law, 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).

This policy is mandatory for all individuals involved in the onboarding and client verification process, including directors, officers, employees, contractors, and any third parties acting on behalf of the Company. A customer is not permitted to make deposits, request withdrawals, or engage in gaming or betting activities until all conditions of acceptance have been satisfied, and the required verification and screening processes have been completed.

2. Scope of the Policy

The provisions of this policy apply to every natural or legal person seeking to establish an account with NUMERETO B.V., regardless of how the registration is initiated. This includes customer registration through the Company's official website, mobile platforms, affiliate arrangements, or through external partner systems.

The policy governs the full customer lifecycle, beginning at the initial stage of registration and continuing throughout all phases of account activity up to account closure or termination. It applies to all services and products offered by NUMERETO B.V. that fall under the scope of its Curaçao gaming license OGL/2024/315/0489.

3. Customer Acceptance Integration

NUMERETO B.V. only accepts customers who meet all relevant legal, regulatory, and internal policy requirements. Each applicant must be verified to confirm that they have reached the legal gambling age, which is eighteen (18) years or older or in accordance with the legal minimum age in their jurisdiction. Furthermore, customers are obligated to submit complete and verifiable personal details, such as full legal name, date and place of birth, nationality, and current residential address.

The Company strictly prohibits the onboarding of customers who reside in, are located in, or are transacting from jurisdictions that are restricted under Curaçao's legal regime, international sanctions programs, or NUMERETO B.V.'s internal list of blocked or high-risk countries. During onboarding, each applicant is screened against sanctions databases maintained by global and regional authorities, such as the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), as well as Curaçao-specific frameworks including the Sanctions National Ordinance and the Kingdom Sanction Act.

Only funds derived from legitimate and identifiable sources are permitted for use within the platform. Where a customer's risk profile warrants further examination, NUMERETO B.V. reserves the right to request additional documentation to validate the origin of funds or, if necessary, the customer's overall source of wealth. The Company may also reject customers with a known history of fraud, chargeback abuse, repeated bonus exploitation, self-exclusion due to gambling addiction, or other regulatory breaches.

4. Risk-Based Approach

NUMERETO B.V. applies a structured Risk-Based Approach (RBA) to the onboarding and ongoing assessment of customers to ensure that all due diligence efforts are proportional to each customer's unique risk level. This methodology enables the Company to implement tailored measures based on various factors such as financial background, product usage, geographical exposure, and the technological methods used to access its services.

Customer Risk Profiling

Every prospective client is evaluated to determine their potential exposure to money laundering, terrorist financing, or proliferation financing risks. Based on this evaluation, the Company assigns an appropriate level of due diligence that matches the customer's risk characteristics.

Clients with transparent financial situations, such as stable employment in low-risk industries and gambling behavior consistent with their declared income, are categorized as low risk. On the other hand, individuals may be classified as high risk if they exhibit indicators such as multiple income sources with limited traceability, occupations in sectors with elevated AML risk (e.g., cryptocurrency), or if their activity does not align with their reported financial capacity. Additionally, Politically Exposed Persons (PEPs), their relatives, and close business associates are automatically treated as high-risk and subject to heightened scrutiny.

High-risk clients are processed under Enhanced Due Diligence (EDD) protocols. This includes stricter verification processes, the collection of additional

documentation, and consistent monitoring throughout the relationship. Some examples of high-risk scenarios that would require EDD are:

- Applicants with irregular or hard-to-verify income, who must submit tax returns, payslips, or business-related records.
- PEPs and their associates, whose onboarding requires sign-off by senior management, proof of wealth and source of funds, and continuous monitoring.
- Customers whose betting activity significantly exceeds their known financial capacity, triggering deeper review and justification.
- Sudden and unexplained changes in gambling patterns or the use of intermediaries in financial transactions.
- Detection of multiple accounts linked to the same user through internal controls and analytics.
- Requests to redeem large amounts without corresponding betting activity, particularly in connection to junket or third-party operators.

To ensure risk profiles remain current, NUMERETO B.V. conducts ongoing reviews and re-evaluates risk classifications when changes occur, such as new jurisdictions, large deposits, or changes in user behavior. When risk levels increase, the Company applies additional safeguards such as EDD, enhanced transaction reviews, and temporary restrictions.

Geographic Risk Assessment

NUMERETO B.V. adopts a comprehensive approach to assessing the risks associated with a customer's location or funding origin. The Company regularly updates its risk models using authoritative sources, such as the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the European Commission's high-risk jurisdictions list, OFAC advisories, the U.S. State Department's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from countries under international sanctions are automatically excluded from onboarding. Clients from jurisdictions categorized as high risk are only onboarded after successful completion of EDD procedures and senior-level review.

High-risk locations typically demonstrate one or more of the following conditions: insufficient enforcement of AML/CTF laws, systemic corruption, known links to

terrorist financing or weapons proliferation, or active sanctions imposed by reputable authorities.

The risk classification process is continuously informed by updated data from FATF, CFATF, OFAC, and the European Commission. If a client resides in or transfers funds from a flagged jurisdiction, the case is escalated to the Compliance Officer, and full EDD procedures are mandatory. This includes comprehensive identity validation, a documented analysis of the client's financial background, and extended monitoring for the duration of the business relationship.

Risk Assessment Workflow

1. The client's country and funding origin are checked against external databases during onboarding.
2. Applicants from low-risk countries proceed under standard due diligence.
3. Applicants from high-risk areas are subject to escalation, EDD, and strict monitoring.
4. Applications from sanctioned jurisdictions are automatically declined and recorded accordingly.
5. The Company updates risk assessments dynamically as new information emerges.

5. Onboarding Procedures

NUMERETO B.V. uses a formalized and well-documented onboarding procedure to ensure that only eligible customers gain access to the platform. New accounts are not activated unless the individual has fulfilled all identity verification and sanctions screening obligations.

During the registration process, the client must provide their full legal name, date and place of birth, nationality, residential address, and a valid identification number, such as a national ID or passport number.

All applicants undergo screening against sanctions and PEP databases through automated tools. Any alert or possible match is verified manually by trained compliance personnel to determine if escalation or rejection is necessary.

Applicants flagged as high risk during the initial review are required to submit supporting documents that validate the legality of their funds and, where applicable, provide a source of wealth. These documents may include:

- Recent bank statements showing income deposits
- Financial statements for business accounts
- Tax returns or audited declarations
- Asset sales agreements or inheritance certificates
- Investment portfolio summaries

This detailed verification framework ensures the platform complies with AML/CTF/CPF requirements and prevents onboarding of customers who could pose a threat to the integrity of the system.

6. Client Identification and Document Verification

NUMERETO B.V. requires identity verification for all persons seeking to establish a business relationship with the Company, including beneficial owners and authorized representatives. The Company must be confident that the individual is legitimate and must collect sufficient evidence to validate their identity.

Minimum Requirements for Identity Documents

Each submitted ID must include:

- Full name
- Complete date of birth
- Unique document number
- Issue date or validity period
- Photograph of the individual
- Signature (if applicable)

Document Quality Requirements

The ID must meet these standards:

- Must remain valid for at least one month after submission
- Must be clear, untampered, and free from damage
- All required personal information must be visible and legible

Upload Guidelines for ID Documents

Photographs or scans must:

- Be in accepted formats such as JPG, JPEG, PNG, or PDF
- Include both front and back where applicable
- Have a file size of at least 100 KB and a resolution of 300 DPI or higher
- Be in color, unaltered, and free from editing software manipulation

Image Authenticity Check

The Company performs authenticity checks to ensure images have not been altered. This process evaluates metadata, compression parameters, and file signatures. The goal is to detect any software tampering, even if the changes are minor or cosmetic.

Document Data Validation

The information extracted from identification documents is cross-referenced with international watchlists and sanctions registries to confirm accuracy.

Proof of Address (PoA) Verification

NUMERETO B.V. implements both face-to-face and remote procedures for verifying a customer's residential address, depending on how the relationship is initiated.

Face-to-Face Verification

When clients are onboarded in person, the appointed Money Laundering Compliance Officer (MLCO) inspects the original address document. A certified true copy is taken and retained as part of the verification record.

Non-Face-to-Face Verification

For remote onboarding, the process requires the customer to upload an image of a valid address document. By default, only documents issued within the last three months are accepted. These documents undergo a multi-step verification process:

- **Authenticity Check:** Each image is automatically analyzed to confirm that it has not been altered. This is done using software that evaluates file metadata, signature structures, and compression characteristics to detect editing tools or anomalies.
- **Integrity Check:** Uploaded address documents are compared to a library of official templates. The check looks for consistent formatting, expected fonts and spacing, the presence of all required fields, and authenticity of inscriptions.
- **Data Extraction and Validation:** Critical details such as the customer's full name, address, and the date of issue are extracted. The address is verified for completeness and validity, with geolocation verification supported by services like Google Maps and OpenStreetMap. This enables the MLCO to visualize the location and assess plausibility.

Accepted Proof of Address Documents

Commonly accepted address documents include:

- Utility bills for electricity, gas, water, or internet
- Bank or credit card statements
- Government correspondence such as pension or welfare notices
- Tax or mortgage statements
- Residential lease agreements
- Letters from recognized authorities or employers confirming the address

The submitted document must contain the individual's name, full residential address, and the issuance date. Both paper and digital versions (e.g., PDF format) are accepted.

Alternative Address Proofs

Documents like passports, ID cards, or driving licenses are accepted only if they clearly show the customer's current address. However, such a document cannot be used for both identity and address verification. A different document must be submitted for each.

Unacceptable Documents

NUMERETO B.V. does not accept the following as valid PoA documentation:

- Outdated statements (older than three months)
- Mobile phone bills
- Insurance documentation
- PO Box addresses
- Receipts or medical bills
- Statements from fintech companies
- Documentation lacking full address or name
- Business addresses on personal accounts

Source of Funds (SoF) and Source of Wealth (SoW)

NUMERETO B.V. applies strict controls to determine the origin of client funds and wealth. This includes establishing the direct source of transaction funds (SoF) and, where necessary, understanding the broader context of the client's financial capacity (SoW). These measures are crucial in high-risk situations, especially during Enhanced Due Diligence.

- **SoF** refers to the origin of the money being deposited or transferred, confirmed via bank statements, tax filings, payroll records, etc.
- **SoW** provides insight into how a customer acquired their wealth — this may include inheritance, sale of assets, or long-term investment gains.

Examples of Accepted Evidence:

Income Category

Supporting Documents

Salary	Recent payslips and matching bank deposits, or audited tax filings
Inheritance	Probate documents and bank statement showing deposit; or solicitor's letter confirming inheritance
Gifts or Donations	Notarized gift letter and deposit evidence, or a formal gift agreement
Savings	Savings or standard bank statements
Government Benefits	Documentation of pension, grants, or allowances and proof of deposit
Business Income	Dividend contracts, audited financials, or tax declarations
Loans/Investments	Formal loan/investment agreements and deposit evidence
Sales Proceeds	Sale contracts, bank deposits, shipping documents, tax returns, or e-shop reports

Every document must show a clear audit trail between the customer's financial activity and the origin of funds.

7. Prohibited Clients and Transactions

To reduce the risk of enabling financial crimes, NUMERETO B.V. restricts specific clients and transactions that present unacceptable risks or violate regulatory frameworks. The Company proactively blocks business relationships in the following scenarios:

Prohibited Business Relationships

- Clients who fail or refuse to provide sufficient identity or background data during onboarding.
- Individuals or entities subject to sanctions as outlined in the Company's Sanctions Policy.
- Financial institutions or shell companies operating without a physical presence or not affiliated with a regulated group.

Criminal Associations

Relationships will be denied or terminated if clients are directly or indirectly involved in any of the following criminal activities:

- Terrorism or related offenses
- Narcotics trafficking
- Human trafficking and smuggling
- Sexual exploitation
- Corruption or tax crimes
- Fraud against the EU budget
- Counterfeiting, cybercrime, and organized crime

High-Risk Entity Types

The Company does not onboard clients connected to:

- Bearer-share structures
- The adult, arms, or narcotics industries
- Sanctioned individuals or entities, including SDNs
- Transactions involving sanctioned funds or unverifiable SoF/SoW

Geographic Restrictions

NUMERETO B.V. prohibits business relationships with individuals or entities based in restricted territories, which include but are not limited to:

Disputed/Unrecognized Territories: Crimea, Donetsk, Luhansk, Kosovo, South Ossetia, Northern Cyprus, Palestine, etc.

Restricted Jurisdictions: Iran, North Korea, Syria, Russia, USA, UK, Germany, Netherlands, Curaçao, and others as listed in the original policy.

8. Enhanced Due Diligence (EDD)

Enhanced Due Diligence procedures are implemented for customers whose profiles suggest a heightened level of risk. This includes individuals identified as Politically Exposed Persons (PEPs), their family members and close associates; persons residing in or transferring funds from high-risk jurisdictions; customers engaged in unusually large or complex transactions; or those whose financial activity does not align with their declared income or business operations.

The EDD process at NUMERETO B.V. involves additional layers of scrutiny compared to standard due diligence. A comprehensive assessment is conducted to verify both the source of the customer's funds and their source of wealth, with all claims supported by credible documentation. These documents may include verified financial statements, public registries, employment verification, property records, tax filings, or independent legal attestations.

For corporate customers, ownership structures are traced using national or international corporate registries, ensuring that both legal and beneficial owners are properly identified and verified.

Approval from senior management is mandatory before proceeding with onboarding of any high-risk individual. In exceptionally sensitive or complex cases, escalation to the Board of Directors may be required for final authorization.

Once onboarded, high-risk clients are subject to ongoing enhanced monitoring. Their transaction activity is evaluated more frequently, thresholds for alerts are set lower, and any deviations from expected patterns prompt immediate reassessment. This approach ensures regulatory compliance while enabling the firm to promptly detect and respond to emerging threats or vulnerabilities associated with high-risk relationships.

Prohibited Client Categories

NUMERETO B.V. will not initiate or will terminate any business relationship with clients who fall under the following classifications:

- Customers who remain anonymous or fail to complete the identity verification process within 30 calendar days.
- Legal entities with unclear beneficial ownership or shell companies without meaningful management presence.
- Individuals or organizations listed on international or national sanctions lists, including those issued by the UN, EU, OFAC, OFSI, or those regulated under the Kingdom Sanction Act.
- Clients located in, or conducting transactions from, countries or territories listed as prohibited under the company's geographic risk framework.
- Underage individuals who do not meet the legal age requirement for gambling.
- Clients known or suspected to be involved in fraud, abuse of promotional offers, identity theft, or other financial crimes.
- Customers using third-party payment methods or anonymous channels without sufficient justification or verification.
- Clients whose sources of funds or wealth cannot be verified or are reasonably believed to be linked to criminal activity.

Rejection and Suspension Triggers

NUMERETO B.V. may immediately reject or suspend a customer application in any of the following scenarios:

a. Documentation Failures

- The customer refuses to provide KYC, proof of address, or required EDD documentation.
- Documents submitted are found to be falsified, altered, or intentionally misleading.
- Verification requirements are not fulfilled within the permitted time frame.

b. Risk Factors

- Positive sanctions match or confirmed high-risk PEP classification that cannot be reasonably managed.
- Reasonable suspicion of involvement in money laundering, terrorism financing, or any other form of organized crime.
- Inability to verify the legitimacy of funds or wealth despite repeated efforts.

c. Behavioural Red Flags

- Transactions that show abrupt spikes in deposit/withdrawal volumes unrelated to declared income.
- Use of multiple accounts, unauthorized third-party payments, or misuse of financial instruments.
- Evidence of collusion, non-genuine gambling behaviour, or any actions aimed at circumventing regulatory controls.

9. Termination of Client Relationship

NUMERETO B.V. reserves the right to terminate any customer relationship at any time when compliance, regulatory, or internal policy requirements justify such an action. Termination may be triggered by the following circumstances:

- The client fails to submit required identity or supporting documents within 30 days of request.
- There is credible suspicion of involvement in money laundering, terrorist financing, or proliferation financing.
- The client is found to be in breach of any applicable laws, regulations, or internal compliance or Responsible Gambling policies.

When termination results from suspected criminal activity, the Company files an immediate report with the Financial Intelligence Unit (FIU), in line with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining client funds are returned via the original deposit method unless otherwise directed by legal or regulatory authorities, such as in the case of asset freezes.

A complete audit trail is maintained for each termination case, including the rationale, supporting evidence, and decisions taken. These records are preserved for a

minimum of five years in accordance with Curaçao's AML/CTF record-keeping requirements.

Common grounds for refusal or termination of the relationship include:

- The customer resides in, or is transacting from, a prohibited jurisdiction.
- Failure to provide timely documentation or disclosure.
- Submission of false or misleading data during onboarding.
- Inability to verify sources of funds or wealth.
- High-risk PEP status that cannot be sufficiently mitigated.
- Evidence of abuse, including fraud, manipulation, or promotional misuse.
- Unauthorized third-party involvement in transactions.
- Exclusion based on Responsible Gambling criteria or self-exclusion requests.
- Unexplained large withdrawals or redemption of chips not linked to actual gambling activity.
- Being underage or below the legal gambling age.

10. Curaçao Legislative Framework

NUMERETO B.V. recognises the importance of aligning its Customer Acceptance Policy (CAP) with the broader obligations set forth under Curaçao's legal framework concerning Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). The CAP integrates all core requirements stemming from:

- 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

- The National Ordinance on Games of Chance (LOK)

The company's customer onboarding and monitoring procedures are embedded in its day-to-day compliance practices, ensuring that risk-based assessments are conducted not only during registration but also throughout the duration of the customer relationship. This ensures that any material change in a client's status — whether financial, behavioral, or jurisdictional — is promptly reviewed and addressed.

All personnel involved in the onboarding, verification, and ongoing risk monitoring processes are required to complete compliance training tailored to Curaçao's legal standards. The training emphasizes how to apply the risk-based approach in practice, identify red flags, and escalate issues to senior compliance officers or management when necessary.

To ensure ongoing effectiveness, the company commissions annual independent audits to assess how well the CAP and associated risk procedures are functioning in practice. These audits examine key areas such as document verification, sanctions screening, Enhanced Due Diligence (EDD), and transaction monitoring. Any deficiencies identified are reported to the Board and corrected within specified timelines.

11. Responsible Gambling Alignment

NUMERETO B.V. ensures that its customer onboarding and acceptance protocols are fully harmonized with the company's Responsible Gambling Policy. The aim is not only to mitigate financial crime but also to protect users from gambling-related harm.

If a customer exhibits behaviour that suggests potential gambling harm — such as depositing funds far beyond their apparent financial means or engaging in excessive, prolonged gameplay — the company immediately evaluates the situation. Appropriate interventions may include setting deposit or bet limits, temporarily suspending the account, or, in more serious cases, permanently restricting access to the platform.

Requests for self-exclusion are processed without delay and are applied universally across all customer accounts linked to that individual. These exclusions are maintained for the full period specified by the customer or as required under applicable regulatory guidelines.

Customer-facing teams receive dedicated training to recognize behavioural indicators that may point to problem gambling. This training is integrated into both

the initial onboarding and continuous monitoring processes to ensure that early intervention can take place when necessary.

12. Governance and Review of the Customer Acceptance Policy

NUMERETO B.V. reviews its Customer Acceptance Policy (CAP) at a minimum once per year to ensure that it remains aligned with current legislation, industry standards, and evolving risk landscapes.

This periodic review also takes into consideration any changes in the company's operational risk exposure, emerging client behavioural patterns, or newly adopted technologies that may introduce new risks. When material updates are needed, they are drafted by the Compliance Officer and submitted to the Board of Directors for formal approval.

Once updates are approved, the company ensures that relevant personnel are promptly informed and trained on the revised procedures. This guarantees uniform and correct implementation of the policy across all operational areas.

13. Record Retention

NUMERETO B.V. retains complete and accurate records of all customer acceptance, onboarding, and risk assessment activities for a minimum period of five years from the date of the termination of the customer relationship.

The types of records maintained include, but are not limited to:

- Identity documents and proof of address
- Source of funds (SoF) and source of wealth (SoW) documentation
- Alerts generated from transaction monitoring
- Internal investigation reports and risk assessments
- Enhanced Due Diligence (EDD) files
- Sanctions and PEP screening logs
- Documentation related to account suspensions, closures, or refusals

All records are securely stored in encrypted digital environments with access restricted to authorized personnel. Access is strictly monitored, and all activity is

logged and reviewed regularly to ensure compliance with data protection rules and internal information security policies.

APPENDIX IV

Employee Screening and Monitoring Program

This Employee Screening Program ("Program") outlines the mandatory standards and procedures governing the vetting, evaluation, and ongoing monitoring of all individuals employed or otherwise engaged by NUMERETO B.V.

This policy has been adopted to ensure full compliance with Regulation V.4 of the CGA AML Guidelines, which requires companies to implement appropriate screening measures for employees both before hiring and throughout the duration of employment.

The company also uses an internal Employee Screening Checklist, which is an integral part of this policy and must be completed for every relevant case to demonstrate compliance with the requirements specified herein.

This policy applies to the following categories:

- All full-time, part-time, temporary, and contract employees.
- Senior Management, the Compliance Officer, and all personnel directly involved in AML and CTF responsibilities.
- Third-party contractors or individuals engaged through outsourcing agreements who perform regulated or sensitive functions.

No person may begin employment or assume duties in a high-risk or sensitive role until all screening measures outlined in this document have been fully and satisfactorily completed.

Screening Requirements

NUMERETO B.V. is committed to ensuring that all personnel are fit, proper, and suitable for their roles. Screening procedures are to be risk-based, proportionate to the responsibilities of the role, and fully documented.

The screening process includes the following four components:

- a) Pre-employment screening
- b) Fit-and-proper assessment (where applicable)

- c) Ongoing screening
- d) Completion of the Employee Screening Checklist

Pre-Employment Screening

The Human Resources (HR) department, in cooperation with the Compliance team, is responsible for performing the following pre-employment checks:

- **Criminal Record Verification:**
A check must be conducted to determine whether the applicant has a criminal history involving dishonesty, fraud, financial crime, money laundering, terrorist financing, or any other conduct incompatible with the ethical and regulatory standards required.
- **Identity Verification:**
Candidates must provide valid, government-issued identification documents. The HR department verifies the authenticity and consistency of the documentation provided.
- **Academic and Professional Credential Verification:**
All educational degrees, professional certificates, licenses, and other job-relevant qualifications must be independently confirmed for authenticity.
- **Employment History Checks:**
Past employment information, including job roles, responsibilities, performance, and any relevant disciplinary matters, must be verified in accordance with legal limitations.
- **Reference Checks:**
At least two professional references must be collected. Any negative or questionable information must be escalated to the Compliance function for evaluation.

No employment offer may be finalized until the Employee Screening Checklist is completed and reviewed.

Fit-and-Proper Assessment

For designated roles, a structured Fit-and-Proper Assessment must be conducted to determine the individual's overall suitability. This evaluation includes the following aspects:

- **Integrity and Personal Reputation:**
The individual must not have any adverse regulatory records, criminal

convictions, or any other issues that raise concerns regarding honesty or professional conduct.

- **Competence and Capability:**

This includes assessing relevant qualifications, technical expertise, prior experience in AML/CTF matters, and the ability to meet regulatory obligations.

- **Financial Soundness:**

If permitted by applicable law, a financial assessment may be conducted, including checks for bankruptcy, insolvency, or other red flags involving financial misconduct.

- **Independence and Conflict of Interest:**

The assessment must also consider the individual's ability to act independently, without real or perceived conflicts of interest.

The completed Fit-and-Proper Assessment form is reviewed by the Compliance team and stored along with the Employee Screening Checklist.

Ongoing Screening and Monitoring

Periodic Screening

Employees in sensitive roles, including those involved in compliance or higher-risk operations, are subject to screening at least once per year. This may include:

- Updated criminal background checks (where permissible)
- Re-evaluation of role-specific suitability
- Review of conduct and performance
- Verification of ongoing independence and absence of conflicts

Trigger-Based Rescreening

Additional screening is required in certain situations, such as:

- Promotion or transfer to a role involving higher sensitivity or regulatory exposure
- Reports or evidence of misconduct or behavioural concerns
- Regulatory changes or other developments that increase the role's risk profile

- External information that raises doubts about the employee's integrity or qualifications

Continuous Monitoring of Conduct

Supervisors and the Compliance team are expected to immediately report any concerns regarding staff behaviour, conduct, or integrity for further review and action.

In all such cases, the Employee Screening Checklist must be updated and securely retained.

Documentation and Record Retention

NUMERETO B.V. must retain accurate and complete documentation of all employee screening activities, including but not limited to:

- Background check reports
- Verified credentials and references
- Fit-and-Proper Assessment forms
- Completed and signed Screening Checklists
- Internal approvals and compliance notes
- Records of any adverse findings and the actions taken in response

All records shall be maintained for at least five years, or longer if required by applicable laws or regulatory frameworks. These records must be readily accessible for inspection by the relevant authorities upon request.

Roles and Responsibilities

Human Resources:

- Manages the pre-employment screening process and maintains relevant records.
- Ensures the Screening Checklist is completed before hiring decisions are finalized.
- Escalates any red flags or concerns to the Compliance Officer.

Compliance Officer:

- Oversees screening processes for roles with AML/CTF-related responsibilities.
- Conducts the Fit-and-Proper Assessments.
- Grants or withholds approval for appointments to sensitive positions.
- Verifies compliance with Regulation V.4 of the CGA AML Guidelines.

Senior Management:

- Ensures that sufficient resources are allocated for screening and compliance.
- Approves any exceptional cases or escalations.
- Periodically reviews compliance reports related to employee integrity and screening.

Enforcement

Failure to comply with the Employee Screening Program, including omissions in checklist completion or lack of proper assessments, may result in disciplinary measures. This may include written warnings, demotion, suspension, or termination of employment, depending on the nature and severity of the non-compliance.

The Company affirms that this Policy is aligned with the requirements set by Regulation V.4 of the CGA AML Guidelines and will continue to review it at least annually to maintain consistency with evolving legal obligations and best practices.

New Employee check-list

Employee: _____

Starting date: _____

1.	Copy of national Identity card or passport	
2.	Work permit (if needed)	
3.	Proof of Residence	
4.	Certificate of clear criminal record	
5.	Non-Bankruptcy letter	
6.	Reference letter from previous employer	
7.	License/certificates	
8.	CV (Curriculum Vitae)	
9.	Good repute questionnaire	
10.	Diploma of high education	
11.	AML and IOM acknowledgement letter	
12.	Privacy Notice	
13.	Induction & Initial Training Policy/Acknowledgement form	
14.	Employment Agreement	