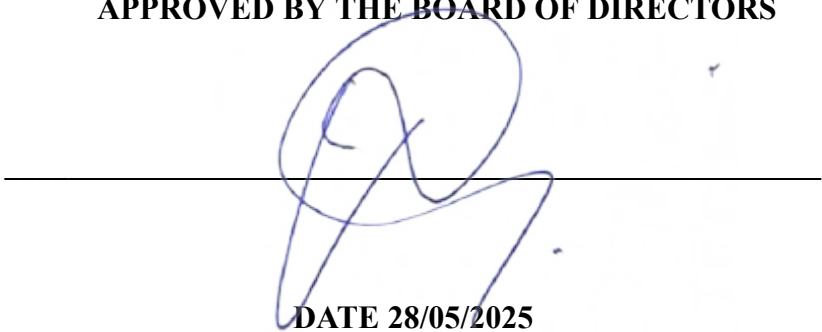


CAECUS N.V.

163779

AML/CTF/CPF POLICY

APPROVED BY THE BOARD OF DIRECTORS



DATE 28/05/2025

Scheduled Review Date: May 2026

Responsible Compliance Officer:

Haris Constantinou
compliance@caecusnv.com

TABLE OF CONTENTS

1. Definitions	4
2. Statement of the Policy	8
3. Overview of the Online Gaming Environment	9
4. Understanding Money Laundering & Terrorism Financing	9
5. Money Laundering, Terrorist Financing, Proliferation Financing	
Risk-Based Approach	11
5.1. Risk Factors	12
5.2. Technological Developments Risk Assessment	15
6. Customer Due Diligence	16
6.1. Conditions for Implementing CDD Measure	16
6.2. Components of the CDD Process	17
6.3. Player Identity Establishment	17
6.4. Understanding Player Relationships	18
6.5. CDD on Existing Customers	18
6.6. Enhanced Investigation for High-Risk Cases	19
6.7. Simplified Verification for Low-Risk Cases	19
6.8. Timing of CDD Measures	19
6.9. Special Considerations for Politically Exposed Persons (PEPs)	21
6.10. Relationship Termination Protocol	21
7. Sanctions Compliance	21
7.1. Monitoring and Reporting Procedures	21
7.2. Client Interaction and Transaction Verification	22
7.3. Continuous Review of Compliance Procedures	22
7.4. Due Diligence and Evasion Prevention	22
7.5. Staff Training and Auditing	22
8. Management Responsibilities	22
8.1. Policy Review and Risk Assessment	23
8.2. Employee Training Programs	23

8.3. Internal Control Framework	23
9. Compliance Officer	23
9.1. Designation and Authority	23
9.2. Key Functions of the Compliance Officer	24
9.3. Core Responsibilities	24
9.4. Conclusion	24
10. Detection and Reporting of Suspicious Activity	25
10.1. Characteristics of Unusual Transactions	25
10.2. Assessment and Reporting Procedures	26
10.3. Confidentiality of Reporting Process	26
11. Audit Procedures	26
11.1. Objectives of the Audit	26
11.2. Auditor Appointment	27
11.3. Adherence to Standards	27
11.4. Audit Reporting	27
11.5. Oversight by the Gaming Control Board	27
11.6. Consequences of Non-Compliance	28
12. Record Keeping	28
13. Training	28
13.1. Role-Specific Training Requirements	29
13.2. Training Structure	29
13.3. Training Curriculum Content	29
13.4. Delivery Methods	29
13.5. Qualified Trainers	29

1. Definitions

Suspicious Activity Report/Suspicious Transaction Report – **SAR/STR**

Counter Proliferation Financing – **CPF**

A senior management member who maintains independence from the games operations, responsible for deterrence and detection of ML/TF/CPF risks – **Compliance Officer**

The Financial Intelligence Unit Curacao, referred to in art. 2 of the Norut – **FIU**

Source of Funds/Wealth – **SOF/SOW**

Know Your Business – **KYB**

The United States – **US**

Office of Foreign Assets Control – **OFAC**

Ultimate Beneficial Owner – **UBO**

Know Your Customer – **KYC**

Customer Due Diligence – **CDD**

Counter Terrorism Financing – **CTF**

Enhanced Due Diligence – **EDD**

Politically Exposed Person – **PEP**

Anti-Money Laundering – **AML**

The Caribbean Financial Action Taskforce (an organization of 24 states of the Caribbean Basin, Central and South America) – **CFATF**

Board of Directors of the Company – **BoD**

The National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63) – **NOOGH**

The European Union – **EU**

The United Nations – **UN**

Financial Action Task Force – **FATF**

The United Kingdom – **UK**

Money Laundering

The act of hiding or masking money obtained through illegal means, typically broken down into three phases: placement (introducing illicit money into the system), layering (obscuring the money's origins through complex transactions), and integration (legitimizing the funds by reintroducing them into the economy).

AML Policy

A strategy aimed at curbing money laundering and terrorism financing, consisting of written internal policies, procedures, and safeguards. It is managed by an AML team, headed by a Money Laundering Reporting Officer (MLRO), who ensures the team receives proper training and organizes external audits of the program.

Anti-Money Laundering and Counter-Financing of Terrorism Program

A set of internal measures and controls to prevent both money laundering and terrorism financing, supervised by the AML team led by the MLRO. This person is responsible for ensuring AML-related training and auditing the program's effectiveness.

Money Laundering Reporting Officer (MLRO)

The person in charge of overseeing anti-money laundering efforts, including filing reports on suspicious transactions and enforcing AML policies and strategies within the organization.

Alert

A signal that prompts further review, triggered by certain predefined red flags or patterns, indicating potential money laundering or suspicious activity.

Beneficial Owner

The individual who has ultimate control or ownership of an account, even if it is managed by another party.

Blacklist

A list of individuals, organizations, or countries flagged for potential sanctions violations. This list is used for compliance purposes and may include internal, government, or vendor-maintained data.

Comprehensive Sanctions

Sanctions that prohibit all forms of interaction or transactions with a specific country, with very few exceptions.

Criminal Proceeds

Assets or funds that are obtained as a direct or indirect result of criminal activities.

Customer

Any individual or entity that opens an account and engages in business transactions with the Company.

Customer Relationship

All interactions between a customer and the Company from the point of onboarding through the entire lifecycle of the customer's engagement with the Company's products or services.

Know Your Customer (KYC)

A process involving the verification of a customer's identity and financial behavior, aimed at detecting unusual or suspicious activities.

Know Your Employee (KYE)

Policies to scrutinize employees to identify conflicts of interest, criminal backgrounds, or suspicious behavior that could pose risks to the company.

Due Diligence

A process of investigation and assessment of a person or entity before entering into a business relationship to ensure no legal, financial, or reputational risks are involved.

Customer Due Diligence (CDD)

Standard internal practices to confirm a customer's identity and evaluate their risk profile. It helps the company ensure compliance with regulations and mitigate risks like fraud and money laundering.

Enhanced Due Diligence (EDD)

Additional scrutiny applied to higher-risk customers, going beyond standard CDD procedures to gain a deeper understanding of their business activities and financial transactions.

High-Risk Third Country

Countries that are flagged by regulatory bodies like the European Commission or FATF due to insufficient measures to prevent money laundering or terrorism financing, thus posing significant risks.

Economic Sanctions

Measures imposed by one or more nations to influence another nation's policies, usually in the form of trade or financial restrictions.

Mandatory Sanctions Lists

Official lists required by law or regulation for organizations to check against when conducting business, such as UN Security Council Resolutions or local sanctions lists.

Egmont Group of Financial Intelligence Units

A global network of financial intelligence units (FIUs) that facilitates cooperation, training, and information-sharing to combat money laundering and terrorist financing.

Embargo

A government-imposed ban on trade or commercial activity with a specific country or product category.

European Union (EU)

A political and economic union of European countries that, among other things, sets regulations for combatting money laundering and terrorism financing across its member states.

Exclusions List

A list maintained by the compliance team containing names that have been cleared and excluded from further sanctions screening.

Financial Action Task Force (FATF)

An international organization that sets global standards for combating money laundering and terrorist financing. It also produces reports on emerging risks and trends in these areas.

Greylist

A list of countries or entities that have been identified as having weak anti-money laundering frameworks, but are working to address deficiencies.

Financial Intelligence Unit (FIU)

A national agency responsible for receiving and analyzing reports of suspicious financial transactions and forwarding them to the appropriate authorities.

First Line of Defense

The initial level of an organization's compliance framework, consisting of employees who interact directly with customers and gather relevant information to ensure proper screening.

Inherent Risk

The level of risk present before any mitigating measures or controls have been applied.

Investigation

The process of examining and gathering information in response to potential violations of sanctions or financial crimes.

Layering

A phase in the money laundering process where illicit funds are moved through various transactions to obscure their origins.

Minor

An individual under the age of 18.

Monitoring

The ongoing review of customer activity to detect unusual patterns or behavior, often aided by automated systems.

Office of Foreign Assets Control (OFAC)

A US Treasury Department agency responsible for administering and enforcing economic sanctions against foreign nations, organizations, and individuals.

Politically Exposed Person (PEP)

An individual in a prominent public position, such as a government official, whose financial transactions may require closer scrutiny due to the potential for corruption or illicit activities.

Red Flag

A warning sign indicating potential suspicious behavior or transactions that warrant further investigation.

Regulatory Agency

A governmental body responsible for overseeing financial institutions, issuing regulations, and enforcing compliance with laws.

2. Statement of the Policy

CAECUS N.V. is dedicated to preventing money laundering and the financing of terrorism through the establishment of this comprehensive AML/CTF/CPF Policy. This policy is aligned with both local and international standards to ensure compliance with all relevant regulations.

The primary objective of this policy is to create a robust framework for managing risks associated with various aspects, including customer interactions, service offerings, payment methods, geographical considerations, and distribution channels.

The Board of Directors (BoD) at CAECUS N.V. holds the responsibility for the approval and implementation of the policy, ensuring that it is effectively executed and monitored for compliance. This policy undergoes an annual review and may be revised as necessary to incorporate significant changes in regulations or operational procedures. Additionally, urgent amendments may be proposed by a designated officer based on recommendations from internal and external AML audits, taking into account any potential risks and impacts.

The AML/CTF/CPF Policy adheres to key legislation in Curacao, which includes the National Ordinance for Games of Chance (LOK), the Criminal Code of Curacao, 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), effective from May 16, 2024. The policy also complies with the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

In addition to local legislation, this policy incorporates international standards and frameworks, such as the Financial Action Task Force (FATF) Recommendations, the European Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs), and the Wolfsberg Principles.

CAECUS N.V. is committed to upholding the standards established by Curaçao's AML/CTF/CPF supervisory authority, the Curaçao Gaming Control Board. All directors, officers, and employees, along with any external consultants engaged for audit purposes, are required to follow and support the principles outlined in this policy.

3. Overview of the Online Gaming Environment

CAECUS N.V., a legally registered entity in Curaçao (Company Number 163779), operates the website <https://1xbet.com/en>. The company is authorized under the license issued by the Curaçao Gaming Control Board to offer games of chance (License Number OGL/2024/1262/0493), identified as, and adheres to the relevant licensing regulations and regional limitations set forth by the Curaçao regulatory authorities. These regulations prohibit remote gaming licensees from providing services to individuals in specific jurisdictions, including the United States, Australia, Dutch West Indies (Aruba and Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. Consequently, CAECUS N.V. focuses its operations exclusively in markets where online gambling is permitted by law and refrains from targeting customers in regions where it is not allowed.

As an e-gaming and betting operator, CAECUS N.V. faces several potential risks related to money laundering. These risks encompass identity theft, fraud, the structuring and layering of transactions, and the possibility of collusion between employees, customers, or external payment service providers aiming to circumvent internal security protocols.

4. Understanding Money Laundering & Terrorism Financing

Money laundering represents a crucial aspect of financially motivated crime that frequently crosses international borders. It is associated with a range of illicit activities, including tax evasion, sanction violations, fraud, corruption, illegal arms trafficking, drug smuggling, extortion, and kidnapping. The primary objective of money laundering is to hide the illegal origins of the proceeds derived from these activities by disguising their identity, source, and intended use.

Stages of Money Laundering

The money laundering process typically unfolds in three distinct stages:

1. **Placement:** This initial step involves injecting illicit funds into the financial system. Common techniques include depositing cash into bank accounts, acquiring valuable assets, or engaging in various financial transactions. The aim is to start blending these funds into the legitimate economy.
2. **Layering:** In this stage, the illicit funds undergo a series of convoluted transactions to obscure their original source. This can involve transferring money between multiple accounts, exchanging currencies, or investing in diverse financial products. The objective is to create a complex network of transactions that obscures the audit trail, making it challenging to trace the money back to its origin.
3. **Integration:** The final stage involves reintegrating the laundered money into the legitimate economy. This can be achieved by purchasing high-value items, investing in

cash-intensive businesses, or participating in other legal financial activities. At this point, the funds appear legitimate and are significantly more difficult to link back to their illegal origins.

Money laundering can occur at various points within this process, and online gambling platforms can be susceptible to misuse during these stages. This emphasizes the necessity for CAECUS N.V. to avoid providing anonymous services or facilitating dubious transactions.

Relationship to Terrorist Financing

Terrorist financing entails the funds used to support terrorist activities. These funds may originate from legitimate sources but are often funneled through financial systems in a manner akin to money laundering. For instance, prepaid cards are often employed to procure materials for terrorist acts. Therefore, it is essential for staff to receive training on current developments in this field.

Risk Management and Compliance Strategies

To mitigate the threats posed by money laundering, CAECUS N.V. prioritizes the identification and management of potential risks. Key strategies include:

- Performing comprehensive customer due diligence to confirm identity documentation, age, and location, addressing issues of fraud and identity theft.
- Vigilantly monitoring for unusual patterns of activity involving multiple accounts or significant transaction volumes to detect irregularities.
- Identifying and addressing deposits originating from illicit activities or used to temporarily hold such funds within the platform.
- Observing player-to-player transfers to prevent misuse of the platform for transferring funds between individuals or cashing out.

This list is not exhaustive, as new risks may arise. The company conducts regular risk assessments tailored to specific concerns and offers ongoing training to employees to enhance its internal anti-money laundering (AML) compliance initiatives.

Terrorism financing encompasses the provision of funds intended to support terrorist activities, sourced from both legal and illegal means. These funds are crucial for executing a range of operations related to terrorism.

The sources of terrorist funding can be divided into two categories: legal and illegal. Legal sources may include legitimate businesses, charitable donations, and lawful financial activities, which terrorists can exploit to channel money through donations and business transactions. In contrast, illegal sources stem from criminal activities such as drug trafficking, fraud, smuggling, and extortion, alongside money laundering tactics that obscure the origins of the funds.

Funds are transferred through a variety of methods. Formal channels involve traditional banking systems and financial institutions, where sophisticated techniques like layering and structuring are utilized to avoid detection. Alternatively, informal channels, such as hawala systems, operate outside regulated financial frameworks, making them more difficult to trace.

Indicators of terrorism financing often manifest as unusual transaction patterns that diverge from standard personal or business behavior. This may include large or frequent transfers to or from high-risk regions and transactions associated with known terrorist affiliates. Furthermore, suspicious activities can surface in high-risk sectors, involving substantial cash transactions or financial actions seemingly designed to conceal terrorist operations.

To effectively combat terrorism financing, robust regulatory and compliance measures are vital. The Anti-Money Laundering (AML) policies of CAECUS N.V. are specifically structured to identify and prevent such activities through customer due diligence (CDD), transaction monitoring, and the reporting of any suspicious activities. The company adheres to various sanctions lists, including but not limited to the Sanctions National Ordinance (SNO, N.G. 2014, no. 55), the Kingdom Sanction Act (N.G. 2016, no. 54), announcements from the Gaming Control Board (GCB), the Office of Foreign Assets Control (OFAC), United Nations Security Council sanctions, EU sanctions, and the U.S. List of Foreign Terrorist Organizations. These lists help ensure that transactions do not inadvertently support terrorism.

Internationally, the Financial Action Task Force (FATF) provides guidelines aimed at addressing money laundering and terrorism financing, stressing the importance of robust policies for detecting and reporting suspicious transactions. The OFAC enforces U.S. economic and trade sanctions and maintains the Specially Designated Nationals (SDN) list, which includes individuals and entities linked to terrorism. The European Union (EU) also enforces regulations designed to prevent the financial system from being misused for terrorist purposes, requiring member states to implement effective AML measures and adhere to international sanctions. Moreover, the United Nations (UN) contributes to global efforts to disrupt terrorist financing by imposing sanctions and maintaining lists of individuals and entities connected to terrorism, thereby limiting the resources available to terrorist groups.

5. Money Laundering, Terrorist Financing, Proliferation Financing Risk-Based Approach

A cornerstone of CAECUS N.V.'s compliance infrastructure is the application of a comprehensive risk-based approach (RBA), which guides its overall risk assessment strategy. This approach entails the systematic evaluation of risks associated with its clientele, products, services, and the jurisdictions in which it operates. By regularly conducting detailed risk assessments, the company enhances its ability to proactively identify, assess, and address vulnerabilities. This strengthens the organization's capacity to detect and respond to emerging threats in full alignment with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulatory requirements.

Following the identification of risk exposure, CAECUS N.V. implements tailored mitigation strategies proportionate to the assessed level of risk. The company applies adaptive compliance measures to protect its platform from financial crime threats, including money laundering, terrorist financing, and proliferation financing.

One of the primary risk control mechanisms adopted is Enhanced Due Diligence (EDD). This includes conducting comprehensive investigations on high-risk customers and transactions by gathering additional information on the origin of funds, verifying the structure of beneficial ownership, and analyzing the customer's financial background. These enhanced procedures significantly improve the company's ability to detect and prevent unlawful financial behavior.

Furthermore, CAECUS N.V. employs advanced transaction monitoring systems capable of detecting suspicious financial activities in real time. These systems are designed to generate automated alerts when atypical transaction patterns are identified—patterns which may be indicative of fraud, money laundering, or terrorist financing. Alert thresholds are carefully defined to ensure that any irregularities are promptly escalated for investigation.

The company also enforces strict customer verification processes, especially in relation to high-risk individuals and entities. Robust identity verification protocols involve cross-checking information against reliable data sources and ongoing monitoring of flagged profiles, ensuring such customers are thoroughly vetted prior to engaging in any financial activity on the platform.

To maintain consistent regulatory compliance, CAECUS N.V. performs regular analysis of transaction data and customer risk profiles. This continuous monitoring process facilitates the timely detection of suspicious activity, the reclassification of customer risk levels, and the adjustment of internal AML/CTF/CPF policies in response to evolving threats or regulatory developments. The company is committed to maintaining a responsive and adaptive compliance framework that evolves alongside emerging financial crime trends.

An essential component of CAECUS N.V.'s risk-based compliance program is the accurate documentation and reporting of relevant data. Suspicious transactions are reported without delay to the appropriate regulatory authorities, in line with applicable legal obligations. Additionally, the company maintains comprehensive records of customer identification details, transactional activity, and risk assessment outcomes for the duration mandated by law. These records are securely stored and readily available for regulatory review, reinforcing the company's dedication to transparency and accountability.

Through the strategic implementation of risk-based controls, CAECUS N.V. affirms its commitment to operating within a secure, transparent, and fully compliant framework. Continuous risk monitoring, policy development, and adherence to international AML/CTF/CPF obligations ensure the integrity of the platform and help guard against financial misconduct. This proactive approach reflects the company's position as a responsible, trustworthy, and fully compliant participant in the iGaming sector.

5.1. Risk Factors

Customer risk pertains to the likelihood of exposure to money laundering (ML) and terrorism financing (TF) through interactions with particular individuals. As part of its risk-based compliance model, CAECUS N.V. conducts thorough evaluations of customer profiles, financial transactions, and sources of wealth to identify potential vulnerabilities.

Certain customer types are considered to carry a higher risk of financial crime involvement. This includes individuals with multiple income streams, which can complicate the verification process of fund legitimacy. Clients with fluctuating or unpredictable financial behavior may also increase the risk due to the challenge in assessing their financial patterns. Politically Exposed Persons (PEPs) are subject to intensified scrutiny owing to their potential influence over public funds and associated corruption risks.

Additional high-risk categories include individuals with substantial and inconsistent spending, whose expenditures appear disproportionate to their declared income, and customers who maintain multiple gaming accounts, potentially to evade monitoring or obscure financial activity. To address these risks, CAECUS N.V. has implemented transaction thresholds that reflect normal customer behavior patterns.

Typically, low-risk individuals are characterized by having a single, verifiable source of income. In contrast, those with multiple income sources, inconsistent spending patterns, or irregular transactions are subject to elevated monitoring and Enhanced Due Diligence (EDD) measures.

Product, Service, and Transaction Risks

Certain gaming services, financial instruments, and transaction types inherently present greater risks of being exploited for money laundering and terrorism financing. Criminal actors often target weak points within gaming ecosystems to manipulate outcomes or obscure the origins of illicit proceeds.

Illicit funds derived from activities such as fraud, narcotics trade, or theft may be funneled through gambling platforms to disguise their origin. The use of anonymous payment tools—such as prepaid cards and digital assets like cryptocurrencies or tokens—presents heightened risks due to limited traceability.

The misuse of player accounts for non-gaming purposes, such as acting as temporary repositories for financial transactions, also raises compliance concerns. Similarly, peer-to-peer transfers among players can facilitate unauthorized movement of funds.

Criminals may attempt to exploit third-party financial instruments, such as bank accounts or cards registered under different identities, or transfer funds across multiple gaming accounts, further complicating traceability. Financial services linked to gambling, such as currency exchanges, credit facilities, or use of multi-operator platforms, present an additional layer of risk.

To counter these threats, **CAECUS N.V.** enforces stringent transaction monitoring protocols, applies EDD processes where appropriate, and maintains full compliance with global AML/CTF/CPF regulations.

Geographical Risk

Geographical risk is determined by the location of a customer and the origin of their financial resources, which may indicate elevated exposure to ML, TF, or Counter-Proliferation Financing (CPF) threats. Jurisdictions associated with weak AML/CFT controls, high corruption levels, or

international sanctions pose heightened risk. Countries identified in relation to terrorism or weapons proliferation are subject to strict oversight.

To evaluate such risks, CAECUS N.V. relies on reputable regulatory and international data sources, including but not limited to:

- Reports from the Financial Action Task Force (FATF), identifying high-risk countries under increased monitoring;
- Caribbean Financial Action Task Force (CFATF) public statements concerning regional financial crime issues;
- U.S. Department of State International Narcotics Control Strategy Reports (INCSR), highlighting financial crime trends;
- The European Commission's list of high-risk third countries with AML/CFT deficiencies;
- Office of Foreign Assets Control (OFAC) sanctions lists targeting terrorism-linked jurisdictions;
- Transparency International's Corruption Perceptions Index (CPI), which ranks countries based on perceived levels of corruption.

CAECUS N.V. applies a structured geographic risk classification methodology to differentiate between high-risk and low-risk countries. Enhanced Due Diligence is employed for users in higher-risk jurisdictions, and financial activity involving sanctioned territories is restricted. Risk classification protocols and monitoring systems are continuously updated to reflect changes in global assessments, ensuring ongoing compliance with AML/CTF/CPF regulations and maintaining a secure, transparent operating environment.

Distribution Channel Risks and Mitigation Measures

The methods by which CAECUS N.V. engages with its customers also introduce potential exposure to money laundering, terrorist financing, and fraudulent activity. Channels that facilitate anonymity—particularly those enabling financial transactions or user interactions without proper identification—pose increased risk if not appropriately controlled.

To mitigate these vulnerabilities, the company enforces advanced verification measures for all customer interactions involving anonymous features. Technological solutions, including biometric authentication and sophisticated identity verification tools, are employed to reduce risks associated with fraud and unverified transactions.

By applying rigorous monitoring procedures and ensuring secure authentication across all distribution points, CAECUS N.V. reinforces its commitment to international compliance

standards and strengthens the security and transparency of its gaming platform against financial crime threats.

5.2. Technological Developments Risk Assessment

CAECUS N.V. is dedicated to ensuring that advancements in technology are not exploited for the purpose of financial crimes such as money laundering (ML) or terrorist financing (TF). As innovation continues to transform the iGaming sector, the company implements robust controls and a proactive risk management framework to identify and mitigate any vulnerabilities associated with technological change. Through the integration of thorough risk evaluation processes, CAECUS N.V. safeguards its compliance obligations across all new business practices, service models, and product innovations.

Procedures for Risk Identification and Assessment

In order to detect and manage risks associated with technological innovation, CAECUS N.V. conducts in-depth assessments in the following scenarios:

- The launch of a new product or feature on the gaming platform;
- The introduction of operational practices aimed at improving efficiency or enhancing user engagement;
- The adoption of novel service delivery mechanisms, including modern payment technologies or digital account access tools;
- The deployment or integration of emerging technologies into current or future gaming infrastructure, such as blockchain solutions, AI-powered services, or advanced cybersecurity protocols.

Prior to implementing any new technology, a comprehensive review is conducted to assess potential vulnerabilities that could be exploited for criminal activity. This process involves identifying and analyzing associated risks and ensuring all findings are thoroughly documented. The assessment is aligned with both domestic and international AML/CTF regulatory frameworks, reinforcing the company's ability to identify, manage, and mitigate technology-driven threats related to financial crime.

Implementation of Risk Mitigation Strategies

Upon identification of potential risks, CAECUS N.V. promptly adopts appropriate mitigation measures to reinforce its defenses against emerging threats. These may include:

- Strengthening of Security Protocols – The implementation of multi-factor authentication (MFA), biometric identity verification, end-to-end data encryption, and artificial intelligence (AI)-based fraud detection tools to safeguard systems from misuse;

- **Enhancement of Transaction Monitoring Capabilities** – Upgrading monitoring platforms to detect atypical financial behavior using automated systems capable of flagging transaction patterns indicative of ML or TF;
- **Policy Adaptation** – Revising AML/CTF policies to address new risk factors introduced by evolving technology. The company ensures that its compliance framework remains agile, keeping pace with the dynamic nature of cybercrime and financial crime techniques.

Through ongoing monitoring and adjustment to technological developments, CAECUS N.V. upholds its commitment to maintaining a secure and compliant operational environment. This forward-looking strategy protects the integrity of the company's financial ecosystem and affirms its alignment with global AML/CTF obligations. By doing so, the company ensures that innovation is not pursued at the expense of regulatory compliance or financial security.

6. Customer Due Diligence

The company is dedicated to maintaining compliance with regulatory standards that prohibit the establishment of anonymous or fictitious accounts within the casino sector. To effectively combat risks related to money laundering, terrorist financing, and proliferation, it is imperative to verify player identities and comprehend their business relationships. A comprehensive Customer Due Diligence (CDD) policy is essential for evaluating risks and ensuring adherence to all regulatory obligations. Any activities deemed suspicious will be reported to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

6.1. Conditions for Implementing CDD Measures

The company will implement CDD measures under the following conditions:

- **Transactions of NAF 4,000 or more:** CDD measures are applied to any single transaction that meets or exceeds this threshold.
- **Occasional transactions exceeding NAF 4,000:** This includes infrequent transactions that surpass the specified limit.
- **Suspicion of illicit activities:** Any indication of money laundering or terrorist financing will trigger CDD protocols.
- **Uncertainties in customer identification:** If previously obtained identification data raises doubts, CDD measures will be activated.
- **Linked transactions:** This applies to either a single transaction or multiple transactions that collectively exceed NAF 4,000. Even if individual transactions are below this threshold, linked transactions will still necessitate CDD. High-risk transactions will require Enhanced Due Diligence (EDD).

6.2. Components of the CDD Process

The company's CDD procedures will encompass the following actions:

- **Identity Verification:** Players will be identified using credible, independent documents or data. This process includes confirming the ultimate beneficial owner of legal entities and understanding their ownership structure.
- **Ongoing Monitoring:** Continuous due diligence will be conducted to monitor transactions, ensuring alignment with the company's understanding of the player and their risk profile, including the source of funds as needed.
- **Confidential Reporting:** Employees are instructed to maintain confidentiality regarding reports made to the FIU, thereby preventing players from being alerted. If suspicions of money laundering or terrorist financing arise, the company will bypass standard CDD processes and report directly to the FIU.

6.3. Player Identity Establishment

To establish a player's identity, the following information will be collected:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number

For low-risk scenarios, only basic information will be required. In higher-risk situations, more detailed information will be collected to mitigate the risks associated with money laundering and terrorist financing.

- **Risk Evaluation:** Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.
- **Verification Methods:** Identity verification will be executed through:
 - Government-issued photo identification (e.g., passport or ID card).
 - Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.
 - Verification of the address through communication methods such as letters, email, or phone.
 - Biometric checks, cross-referencing database information, IP addresses, and funding methods.

If initial information is insufficient, further verification steps may include requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

6.4. Understanding Player Relationships

The company will seek to identify the purpose and nature of its relationships with players as part of the CDD process. While some relationships may be clear, the company will gather sufficient information to detect any unusual or suspicious activities. For higher-risk clients, detailed documentation of their source of wealth and expected activity levels will be collected to ensure legitimacy. For lower and medium-risk players, basic employment or business information will suffice, supplemented by independent verification for higher-risk individuals.

6.5. CDD on Existing Customers

CAECUS N.V. applies Customer Due Diligence (CDD) procedures not only during the onboarding of new customers but also throughout the lifecycle of existing client relationships. By incorporating ongoing monitoring and periodic risk assessments, the company ensures continued adherence to its regulatory obligations under AML, CTF, and CPF frameworks. This approach is embedded within a broader risk-based compliance strategy aimed at identifying and addressing evolving threats.

Continuous CDD Review and Monitoring

- **Ongoing Due Diligence**
The company consistently applies CDD protocols to all existing customers, with an emphasis on continuous transaction monitoring and the reassessment of risk levels.
- **Risk-Based Application**
For customers whose initial CDD measures were insufficient or incomplete, CAECUS N.V. adopts a retrospective due diligence strategy. This includes:
 - Reassessing and updating CDD records for customers identified as higher risk;
 - Performing scheduled updates to ensure that all customer data remains aligned with AML/CTF/CPF compliance standards.

Circumstances Requiring Reapplication of CDD

The company reevaluates existing clients and re-applies CDD measures under the following conditions:

- A material change in the customer's risk profile, such as large or unexpected transactions, jurisdictional changes, or becoming classified as a Politically Exposed Person (PEP);
- Amendments to legal or regulatory requirements necessitating updated customer information;
- When a customer, previously onboarded, initiates transactions equal to or exceeding the NAF 4,000 threshold, which triggers full CDD verification under the company's policy.

Addressing Gaps in Historical CDD

In instances where customers were initially onboarded without the application of full CDD procedures, CAECUS N.V. takes the following steps:

- Prioritizes high-risk customers for immediate verification;
- Applies comprehensive CDD measures at appropriate intervals based on the customer's risk classification.

By maintaining updated and complete due diligence records for all clients, CAECUS N.V. reinforces its commitment to regulatory compliance, safeguards against financial crime, and contributes to the integrity and security of the gaming environment.

6.6. Enhanced Investigation for High-Risk Cases

In high-risk scenarios, the company will apply Enhanced Due Diligence (EDD) measures, which include:

- Comprehensive investigations into the player's background.
- Verification of sources of funds and wealth.
- Detailed examinations of transaction patterns.
- Regular updates of identification information.

EDD measures will be particularly relevant for politically exposed persons (PEPs), necessitating thorough risk assessments and continuous monitoring.

6.7. Simplified Verification for Low-Risk Cases

For low-risk scenarios, Simplified Due Diligence (SDD) measures will be implemented, which involve gathering basic customer information and conducting less frequent reviews. Although SDD streamlines the process, enhanced measures will be enacted if suspicious activities arise or if the player's risk profile changes.

6.8. Timing of CDD Measures

CAECUS N.V. applies Customer Due Diligence (CDD) measures promptly and in strict accordance with applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations, ensuring the effective identification and verification of customers.

CDD Triggered by Transaction Thresholds

Upon account creation, the company collects and verifies essential identifying information from each player, including:

- Full legal name
- Residential address
- Date of birth
- Politically Exposed Person (PEP) screening
- Sanctions list screening

In accordance with its risk-based methodology, CAECUS N.V. performs identity verification before processing any financial transaction that equals or exceeds NAF 4,000. This requirement applies to:

- A single transaction reaching or exceeding the NAF 4,000 threshold;
- Multiple linked transactions (e.g., deposits, withdrawals, or peer-to-peer transfers) that cumulatively total NAF 4,000.

To maintain a proactive compliance posture, the company tracks and aggregates daily transaction data for each customer, taking into account all activity since the initiation of the business relationship.

When the threshold is met, a complete customer risk assessment is performed, and any outstanding CDD obligations are fulfilled without delay.

Early Completion of Customer Due Diligence

CAECUS N.V. prioritizes the early execution of CDD processes. Full identity verification is conducted during account registration, regardless of whether the financial threshold has been reached. This practice minimizes the risk of illicit funds entering the system before proper due diligence is completed.

Transaction Restrictions for Pending CDD

Should a player reach the NAF 4,000 threshold prior to completing full CDD, the following restrictions are implemented to ensure compliance:

- If the threshold is met through a deposit, the user is restricted from initiating further deposits or withdrawals but may continue to use existing account funds for gaming purposes.
- If the threshold is reached due to a withdrawal request, the account is temporarily frozen, and all gaming activity is suspended until the verification process is completed.

Non-Compliance with CDD Requirements

If a player fails to provide the necessary CDD documentation within 30 days of reaching the NAF 4,000 threshold, CAECUS N.V. proceeds as follows:

- The business relationship with the player is terminated;
- If there is any indication of money laundering or terrorist financing, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU);
- In the absence of suspicion, the remaining funds are returned to the original funding source (bank account or digital wallet);
- If ML/TF suspicion persists, the company follows its internal procedures to determine whether funds should be frozen, ensuring full regulatory compliance.

Managing Tipping-Off Risks

Acknowledging that account restrictions or closures may inadvertently alert a customer, CAECUS N.V. carefully assesses each situation to avoid violating anti-tipping-off provisions under AML/CTF legislation. Internal guidelines direct staff on how to respond appropriately while maintaining regulatory integrity.

Through the timely implementation of Customer Due Diligence measures, CAECUS N.V. ensures full compliance with AML/CTF/CPF obligations, mitigates financial crime risk, and upholds the integrity and transparency of its operations across both digital and physical gaming platforms.

6.9. Special Considerations for Politically Exposed Persons (PEPs)

The company's AML/CTF/CPF policy will require heightened scrutiny of PEPs, their family members, and close associates. EDD measures for these individuals will include obtaining senior management approval, understanding the source of funds and wealth, and conducting rigorous ongoing monitoring.

6.9. Relationship Termination Protocol

The company reserves the right to terminate relationships with players engaged in suspicious activities or those who fail to provide sufficient information. Such decisions must be documented and approved by senior management. Upon termination, all activities will be reviewed, and any suspicious transactions will be reported to the FIU. Records related to terminated relationships will be securely stored for a minimum of five years.

7. Sanctions Compliance

The company is firmly committed to adhering to both international sanctions and regulatory standards as part of our Anti-Money Laundering, Counter-Terrorist Financing, and Proliferation Financing (AML/CTF/CPF) policy. To fulfill these obligations, we have established comprehensive procedures designed to ensure compliance with all sanctions imposed by national and international authorities. This includes conducting thorough due diligence on every client and transaction to prevent any interactions with sanctioned individuals, entities, or regions.

7.1. Monitoring and Reporting Procedures

Monitoring and reporting are vital components of our sanctions compliance efforts. The company continuously scrutinizes all transactions for any suspicious activities that could violate sanctions. Any irregularities identified will be promptly reported to the appropriate authorities. Additionally, our commitment to compliance is bolstered by ongoing training for all personnel, ensuring that they remain informed about current sanctions regulations. This proactive approach helps safeguard our operations and mitigate potential risks associated with sanctions violations.

7.2. Client Interaction and Transaction Verification

To maintain the integrity of our operations, all client interactions and transactions undergo meticulous checks against the latest Sanctions Lists. Automated systems facilitate real-time verifications, and our database is regularly updated to reflect current sanctions information. If a match or suspicious activity is detected, it will be reported immediately to the relevant authorities. The company will take decisive actions, including freezing accounts or blocking transactions, to manage compliance risks effectively.

7.3. Continuous Review of Compliance Procedures

Our sanctions compliance procedures are subject to regular reviews and updates to align with evolving legislation and best practices. This includes ongoing monitoring of the following lists:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- GCB announcements
- EU Sanctions
- UK OFSI Sanctions
- UN Security Council Consolidated List
- US List of Foreign Terrorist Organizations
- OFAC Sanctions

7.4. Due Diligence and Evasion Prevention

Our due diligence efforts are specifically designed to uncover any indirect or covert attempts to engage with sanctioned parties or jurisdictions. If any evasion tactics are identified, they will be reported immediately to the relevant authorities, and corrective actions—including transaction suspensions and account reviews—will be implemented without delay.

7.5. Staff Training and Auditing

Regular audits and continuous training for staff are critical to ensuring that the company remains vigilant and compliant with the latest legislative requirements. This ongoing education helps reinforce our commitment to preventing sanctions evasion and maintaining a robust compliance framework.

8. Management Responsibilities

Senior management plays a crucial role in assessing and managing the risks associated with Anti-Money Laundering, Counter-Terrorist Financing, and Proliferation Financing (AML/CTF/CPF) within the company. To ensure effective oversight, the Board of Directors mandates that the appointed AML/CTF/CPF Officer provides regular updates regarding significant changes or challenges within the control environment. This officer is also responsible

for preparing an annual report that evaluates the effectiveness of the company's measures and controls aimed at mitigating risks related to money laundering, terrorist financing, and proliferation financing.

8.1. Policy Review and Risk Assessment

Senior management is accountable for conducting comprehensive reviews of all relevant policies and procedures at least once each year. These reviews are guided by monthly risk assessments, enabling the identification and timely addressing of any potential vulnerabilities in internal controls and risk management practices. If any deficiencies are identified, the AML/CTF/CPF Officer can recommend necessary adjustments to the Board for approval, thus enhancing the company's risk management and compliance framework.

8.2. Employee Training Programs

In alignment with global best practices, senior management is responsible for overseeing the creation and execution of extensive employee training programs. These initiatives are designed to increase awareness and understanding of AML/CTF/CPF risks among all employees, especially those in critical roles, ensuring they are equipped to effectively recognize and respond to suspicious activities.

8.3. Internal Control Framework

Senior management also ensures that the company maintains a robust internal control framework. This includes establishing adequate segregation of duties, implementing clear authorization processes, conducting ongoing monitoring, and ensuring thorough documentation. To uphold regulatory compliance and enhance the effectiveness of the AML/CTF/CPF program, regular independent audits and assessments are performed to provide objective evaluations and identify areas for improvement.

9. Compliance Officer

9.1. Designation and Authority

The company appoints a qualified individual to serve as the Compliance Officer, a key element of our Anti-Money Laundering (AML) strategy. This appointment is made by senior management to guarantee the role's independence and authority. The Compliance Officer possesses extensive expertise in AML compliance and occupies a senior position, enabling them to effectively oversee the implementation of AML policies and procedures. Their role is formally established through an appointment letter outlining their responsibilities and the organizational reporting structure.

9.2. Key Functions of the Compliance Officer

The Compliance Officer is tasked with several critical functions to ensure the effectiveness of our AML program. These primary duties include:

- **Policy Implementation:** Overseeing the execution of AML policies and procedures to ensure alignment with current regulations.
- **Central Point of Contact:** Serving as the main contact for all AML-related issues.
- **Policy Review:** Regularly reviewing and updating AML policies to address evolving regulatory standards and emerging risks.
- **Training Oversight:** Managing the AML training program to ensure employees are adequately informed about AML requirements and their roles in maintaining compliance.

9.3. Core Responsibilities

The Compliance Officer is entrusted with several essential responsibilities:

- **Transaction Monitoring and Reporting:** Continuously analyzing transactions and client activities to identify suspicious behavior. They are responsible for filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) when necessary and maintaining accurate records of these reports.
- **Policy Development and Updates:** Crafting and revising AML policies and procedures to adhere to the latest Curaçao gaming regulations and international best practices. This includes adapting the AML framework to address new risks and regulatory changes.
- **Employee Training and Awareness:** Ensuring that all staff receive comprehensive AML training and understand their responsibilities in detecting and reporting suspicious activities. The Compliance Officer must regularly update training materials to reflect legislative or policy changes.
- **Regulatory Liaison:** Acting as the primary contact with regulatory bodies, law enforcement, and other relevant authorities on AML matters. This includes responding to information requests and participating in regulatory inspections or audits.
- **Compliance Audits:** Conducting regular reviews and audits of the AML program to evaluate its effectiveness and compliance with legal requirements. The Compliance Officer is responsible for addressing any identified issues and implementing necessary corrective measures.
- **Record-Keeping:** Maintaining detailed records of all AML-related activities, including SARs, internal reports, training sessions, and policy updates. These records must comply with legal requirements and be readily available for regulatory review.

9.4. Conclusion

Through the execution of these functions and responsibilities, the Compliance Officer plays a vital role in safeguarding the organization against money laundering and terrorist financing risks, ensuring rigorous compliance with Curaçao's AML regulations.

10. Detection and Reporting of Suspicious Activity

CAECUS N.V. is committed to recognizing and reporting any suspicious activities that may suggest possible money laundering or terrorist financing. Such activities may include unusual patterns in a client's behavior, frequent high-value transactions, or interactions with high-risk jurisdictions. All employees are encouraged to be vigilant and promptly report any irregularities to the designated Compliance Officer, who will conduct a comprehensive investigation to determine if further action or reporting to the appropriate authorities is necessary.

10.1. Characteristics of Unusual Transactions

Unusual transactions are identified by marked departures from a client's typical business practices or financial profile. Examples may include unexpectedly large transactions, dealings with unknown entities, or transactions that lack a legitimate economic or lawful purpose. Employees use transaction monitoring systems to detect these anomalies and escalate them to the Compliance Officer for further analysis.

The following categories of transactions or intended transactions are considered unusual under the regulatory framework applicable to CAECUS N.V., and may warrant further investigation or reporting to the appropriate authorities:

Transactions reported in connection with money laundering or terrorist financing:

Any transaction that has been reported to law enforcement authorities, such as the Police or the Department of Justice, due to suspected involvement in money laundering (ML) or terrorist financing (TF), is classified as unusual.

Transactions involving sanctioned individuals or entities:

Any transaction conducted by or on behalf of a natural person, legal entity, group, or organization listed under the Sanctions National Ordinance (N.G. 2014 no. 55) is deemed unusual. This includes entities subject to sanctions as published by the competent national authority.

Transactions involving amounts equal to or exceeding NAF 5,000:

Regardless of the method of payment—whether in cash, by check, via electronic means, or other non-physical methods—transactions at or above this monetary threshold are treated as unusual. Specific examples include, but are not limited to:

1. Deposits or withdrawals of NAF 5,000 or more:
The acceptance or disbursement of funds at the request of a client in amounts meeting or exceeding the stated threshold.
2. Purchase of chips totaling NAF 5,000 or more:
This includes, but is not limited to, the acquisition of gaming chips, tokens, or digital gaming credits.

3. Payout transactions of NAF 5,000 or more:

Any payment redemption or payout meeting or surpassing this value is to be treated as unusual.

A transaction may constitute a single event or a series, combination, or pattern of transactions that together total the equivalent of NAF 5,000 or more within a single gaming day. Such cumulative activity is assessed collectively for classification purposes.

Transactions with indications of money laundering or terrorist financing:

Any transaction where there is reasonable cause to believe—or where indicators suggest—that the activity may be linked to money laundering or the financing of terrorism, is to be treated as presumed ML/TF and therefore considered unusual.

10.2. Assessment and Reporting Procedures

Upon receiving reports of unusual transactions, the Compliance Officer will evaluate these activities against established risk indicators and legal standards to ascertain whether they are suspicious. If warranted, the Compliance Officer will submit a report to the Financial Intelligence Unit (FIU) in accordance with Curaçao's anti-money laundering regulations.

10.3. Confidentiality of Reporting Process

To uphold the integrity of the reporting process and comply with legal mandates, CAECUS N.V. enforces a strict policy prohibiting the disclosure of any information pertaining to Suspicious Activity Reports (SARs) to the subjects of these reports or to unauthorized individuals. This confidentiality is essential to prevent any interference with ongoing investigations or legal proceedings. Employees are required to handle all communications regarding SARs with utmost discretion, discussing such matters only with the Compliance Officer or authorized personnel. Any violation of this confidentiality policy is regarded as a serious breach of the company's anti-money laundering framework and may lead to disciplinary actions. This rigorous policy ensures that the reporting process remains confidential and effective in mitigating potential risks to the organization.

11. Audit Procedures

To comply with the updated gaming regulations in Curaçao, CAECUS N.V. conducts an independent audit focused on Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF). This section details the audit process, highlighting the responsibilities of the independent auditor and the review conducted by the Gaming Control Board.

11.1. Objectives of the Audit

The primary aim of the annual AML/CTF/CPF audit is to evaluate the effectiveness and compliance of the company's AML/CTF/CPF practices. This audit is crucial for ensuring

adherence to current legal standards and best practices designed to mitigate risks related to money laundering and terrorist financing. The audit encompasses a thorough examination of the AML/CTF/CPF program, which includes risk assessments, transaction monitoring, staff training, and reporting procedures.

11.2. Auditor Appointment

CAECUS N.V. appoints either an external auditor or an internal audit team with the necessary resources and expertise in AML/CTF/CPF. To avoid any conflicts of interest, this auditor operates independently from the company's AML Compliance team. The company carefully assesses the auditor's credentials, experience, and industry reputation. Additionally, the selected auditor must receive approval from the Gaming Control Board to ensure compliance with Curaçao's gaming regulations.

11.3. Adherence to Standards

The audit process follows international standards and specific requirements set forth by the Gaming Control Board. Key elements of the audit process include:

- **Evaluation of AML/CTF/CPF Policies and Procedures:** Confirming that policies are up-to-date and compliant with legal standards.
- **Risk Management Assessment:** Analyzing the effectiveness of risk assessments and mitigation strategies.
- **Transaction Monitoring Review:** Evaluating the efficiency of systems used to detect and report suspicious activities.
- **Staff Training Evaluation:** Assessing the adequacy and effectiveness of employee training programs.
- **Reporting Mechanism Audit:** Reviewing procedures for reporting suspicious transactions and compliance issues.
- **Customer File Review:** Ensuring adherence to KYC (Know Your Customer), KYB (Know Your Business), and CDD (Customer Due Diligence) protocols.

11.4. Audit Reporting

Following the audit, the independent auditor prepares a detailed report summarizing their findings, recommendations, and any issues identified. This report is submitted to the company's senior management and the Gaming Control Board. CAECUS N.V. is committed to addressing the auditor's recommendations and implementing corrective actions within an established timeframe. Follow-up audits may be required to ensure that corrective measures are effectively executed.

11.5. Oversight by the Gaming Control Board

The Gaming Control Board oversees AML/CTF/CPF compliance for all licensed operators, including reviewing audit results and conducting its evaluations. CAECUS N.V. understands that the Board has the authority to request additional documents, perform inspections, and review the implementation of audit recommendations.

11.6. Consequences of Non-Compliance

The company acknowledges that non-compliance identified through audit results or Board evaluations may lead to penalties, including fines, operational restrictions, or even the suspension or revocation of its gaming license. Therefore, CAECUS N.V. is dedicated to collaborating closely with the Gaming Control Board to implement corrective actions and maintain compliance, thereby preventing future complications.

12. Record Keeping

To adhere to stringent record-keeping standards, our company implements robust procedures for managing documentation associated with AML/CTF/CPF. We maintain comprehensive records, which include customer identification information, transaction details, suspicious activity reports (SARs), training logs, and audit records, all preserved for a minimum of five years.

We ensure the security of these records through advanced encryption techniques and strict access controls to prevent unauthorized access. Regular audits are conducted to verify the integrity of the data and safeguard against potential breaches.

A systematic approach is adopted for organizing records, allowing for efficient retrieval by authorized personnel and regulatory bodies. We conduct continuous internal monitoring and periodic audits to ensure compliance with established protocols.

By effectively managing our records, the company not only meets regulatory requirements but also facilitates auditing processes and contributes to the overall integrity of the gaming industry.

13. Training

CAECUS N.V. has implemented a comprehensive training program focused on Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) for all employees. The primary objective of this training is to equip staff with the essential knowledge and skills needed to detect and prevent activities related to money laundering and terrorist financing. Employees are educated on their legal responsibilities, trained to identify suspicious behaviors, and familiarized with the reporting procedures. A well-informed workforce is crucial for effectively executing AML/CTF/CPF policies, which uphold the integrity and credibility of the gaming industry.

13.1. Role-Specific Training Requirements

The training is tailored to address the specific needs of different roles within the organization and is mandatory for all personnel, including senior management, compliance officers, customer-facing staff, and operational teams involved in financial transactions.

13.2. Training Structure

New employees undergo an extensive initial training program, while all staff members participate in refresher courses at least once a year. Employees in high-risk roles may receive additional training sessions more frequently to ensure they are adequately prepared.

13.3. Training Curriculum Content

The training curriculum covers essential topics, including:

- **AML/CTF/CPF Laws and Regulations:** Specific to Curaçao.
- **Internal Policies:** Overview of CAECUS N.V.'s policies and procedures.
- **Compliance Roles:** Understanding the roles employees play in maintaining compliance.
- **Customer Identification and Verification:** Including KYC (Know Your Customer) and CDD (Customer Due Diligence) processes.
- **Reporting Suspicious Activities:** Guidelines on identifying and reporting suspicious behaviors.
- **Record-Keeping Requirements:** Understanding documentation and record-keeping standards.
- **Implications of Non-Compliance:** Exploring the consequences of failing to comply.
- **Emerging Trends:** Keeping up with trends in money laundering and terrorist financing.

13.4. Delivery Methods

To ensure the training is engaging and effective, CAECUS N.V. utilizes various delivery methods, such as in-person workshops, online courses, interactive e-learning modules, and practical exercises like case studies and role-playing scenarios. This multifaceted approach accommodates different learning styles and reinforces key concepts.

13.5. Qualified Trainers

Training sessions are led by qualified professionals, including internal compliance officers and external consultants, to ensure that the content remains current and relevant, accurately reflecting the latest developments in AML/CTF/CPF compliance.