



## **POLICY**

**for Prevention and Combatting of Money  
Laundering, Terrorist Financing and  
Counter-Proliferation Financing**

**NEXUS INTERNATIONAL ENTERTAINMENT  
N.V.**

**Approved by the Board of Directors**

**February 2025**

Confidential

| Version N         | Approved By            | Prepared by                                                                 |
|-------------------|------------------------|-----------------------------------------------------------------------------|
| 1.1<br>26/02/2024 | The Board of Directors | Compliance officer:<br>Semen Klyuchyk<br>compliance@nexusinternational.tech |
| 1.2<br>28/02/2025 | The Board of Directors | Compliance officer:<br>Semen Klyuchyk<br>compliance@nexusinternational.tech |

In witness thereof,  
the Director has caused this Policy to be signed on February 28, 2025

Signature

05/19/2026



## **TABLE OF CONTENTS**

### **1. Policy Statement**

### **2. Policy Overview**

### **3. Risk assessment**

#### 3.1. Money Laundering

#### 3.2. Terrorist Financing

#### 3.3. Proliferation Financing

#### 3.4. Risk-based Approach

### **4. Customer Due Diligence**

#### 4.1. CDD Measures

#### 4.2. Identification and Verification

#### 4.3. Establishing and Understanding Relationships

#### 4.4. Ongoing Monitoring

#### 4.5. Enhanced Due Diligence, Simplified Due Diligence and PEP's

#### 4.6. Relationship Termination

#### 4.7. CDD Timing

### **5. Suspicious Activity Reporting**

### **6. Sanctions Compliance and Monitoring**

### **7. Senior Management**

### **8. Compliance Function**

### **9. Audit Function**

### **10. Employee Training Program**

### **11. Record Keeping**

## 1. Policy Statement

The purpose of the Anti-Money-Laundering Policy (the AML Policy) is to combat money laundering and terrorism financing, implement best AML/CFT industry standards, and promote company-wide compliance with the local and international Anti-Money Laundering/ Counter Terrorism Financing (AML/CFT) legislation. The AML Policy's uniform framework is based on robust AML/ CFT measures, including the identification and mitigation of the inherent risks associated with customers, products and services, payment methods, countries, and delivery channels.

The design, implementation, and monitoring of the AML policy's framework is approved by the Nexus International Entertainment N.V. Directors (BoD) and is subject to an annual review. In addition to the annual review process, the AML Policy may be amended from time to time to reflect material changes in the AML/CFT legislation or operator practices. Furthermore, a nominated officer may put forward suggestions to implement urgent internal and third- party AML audit recommendations as regards risk probability and risk impact.

First and foremost, the AML Policy is a reflection of the main international objectives highlighted by the current AML/ CTF legislation in Curacao i.e. the upcoming National Ordinance for Games of Chance (LOK), the Criminal Code of Curacao, The National Ordinance on Offshore Games of Hazard ( PB 1993, no.63) ( NOOGH) as well as National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification of clients when Rendering Services (NOIS). ). The AML Policy also reflects the international legislation and policy initiatives such as Recommendations of the Financial Action Task Force (The FATF Recommendations), the European Anti-Money Laundering Directives (the 4th, 5th and the 6th AMLDs), and the Wolfsberg Principles.

As of January, 2025, new regulations for combating money laundering, the financing of terrorism, and the proliferation of weapons of mass destruction have become applicable to online casinos in Curaçao. New regulations are effective as of January 9, 2025. Non- compliance with these regulations can result in severe administrative

and criminal sanctions, underscoring the seriousness with which Curaçao authorities are approaching AML/CFT enforcement

The AML/CFT/CFP Regulations are aligned with the FATF Recommendations, alongside the various AML/CFT/CFP legislations in Curacao.

To summarize, the AML Policy was drafted with the view of complying with the recommendations of the AML/CFT supervisor in Curacao, namely the Curacao Gaming Control Board. The Company's directors, officers, and personnel are committed to upholding the set of standards set in the Policy. The Policy applies to all persons at all levels working for the Company and third-party consultants whose services are enlisted from time to time for audit purposes.

## 2. Policy Overview

Nexus International Entertainment N.V. is a Curacao-based legal entity which currently runs the following websites: [www.luckypari.com](http://www.luckypari.com)

Nexus International Entertainment N.V registered No. 162180 at Abraham de Veerstraat 1, Willemsatd, Curaçao under an application, OGL/2024/1324/0750, for a gaming license in progress with the Curaçao Gaming Control Board. Until that process is concluded, based on a transitional arrangement, the company is permitted to continue its operations under temporary Certificate of Operation issued by the GCB to continue operations. Certificate of Operation is subject to the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, P.B. 1993, no. 63) (NOOGH).

It therefore complies with the licensing requirements as well as regional operational restrictions imposed on it by the Curacao regulatory authorities which explicitly bans their remote gaming licenses from offering their services in the US, Australia, Dutch West Indies (Aruba, Bonaire), Curacao, France, Germany, the UK, Belize, and the Netherlands. The Company only operates in markets where it is permitted to operate and does not solicit customers from those jurisdictions where online gambling is explicitly banned i.e. Qatar or where it is imperative to have a locally obtained permit/license.

Overall, gaming and betting operators are susceptible to the money laundering risks spanning identity theft and fraud, structuring, layering and collusion of the employees with the customers or the external payment providers to help them bypass internal safeguards.

The Company implements a **formal Customer Acceptance Policy (CAP)** as part of its risk-based approach to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF). This policy ensures that all prospective customers are subject to a documented Customer Risk Assessment (CRA) prior to onboarding, evaluating factors such as geographic origin, nature of business, source of funds and wealth, transaction behavior, delivery channel, and whether the individual is a Politically Exposed Person (PEP) or appears on any sanctions or watchlists. Based on this assessment, customers are classified into low, medium, or high risk categories. High-risk customers require Enhanced Due Diligence (EDD), including detailed verification of source of funds, ongoing transaction monitoring, and approval from senior management prior to account activation. The Company prohibits onboarding or retaining customers who are unwilling or unable to complete due diligence requirements, provide false or misleading information, or present an unacceptable level of financial crime risk. The CAP is reviewed annually by the Compliance Officer and is designed to ensure compliance with Curaçao regulatory requirements, FATF standards, and the integrity of the Company's gaming operations.

### **3. Risk Assessment**

#### **3.1 Money-Laundering**

Organized crime operations are based on money laundering, often on an international scale. The illegal origin of criminal proceeds from such crimes as financial fraud, tax evasion, violations of sanctions, bribery, illegal arms trade, drug trafficking, extortion, kidnapping etc. is disguised during its processing, including their identity, source and the destination and equals money-laundering. Therefore, the goal of money-laundering is to make the criminal proceeds appear legitimate from the time the money is placed into the financial system ( placement stage), layered in order to hide the audit trail through the web of complex financial transactions at various financial institutions ( the layering stage), to the time it is integrated back into the financial system through the purchase of luxury items or cash-intensive businesses (integration stage). Money-laundering has social, economic, legal and regulatory implications on the world economy and leads to increasing costs of monitoring businesses from a compliance standpoint.

The gambling and betting industry therefore is considered high risk since online platforms are vulnerable to money-launderers since online gambling transactions are cross-border and services are often anonymous in a non- face-to-face business. VIP

accounts, money services businesses and multiple accounts are just a few challenges that the industry is known for.

Based on the results of the complex business risk assessments, Nexus International Entertainment N.V.'s main priority is to detect and deter money laundering threats as well as mitigate such risks in the following areas:

Using the online platform as a player-to-player transfer route to funnel funds between sellers and buyers and cashing out when necessary.

Depositing funds obtained from illicit operations and/or using the online platform as "parking", rather than with the goal of engaging in online gambling or online sports betting.

Verification fraud and identity theft (customer due diligence covering documentation verification, age verification and location verification)

Operation of multiple accounts and high transaction volumes

This list is not exhaustive and whereas additional risks may materialize from time to time, the Company implements robust KYC procedures to identify high-risk customers, utilizes advanced proprietary software to detect suspicious transaction patterns, offers regular AML trainings to the employees, and conducts regular audits of AML controls and systems.

### **3.2 Terrorism- Financing**

Providing funds via different methods and sources for carrying out terrorist activities defines the term terrorism financing, including but not limited to direct funding for the planning and execution of terrorist acts or financial support enabling terrorism such as training, recruitment, and propaganda. Money laundering and terrorism financing are two separate crimes which, nevertheless, are often mentioned together. Countering the financing of terrorism is as important as combating money-laundering but its pattern is largely different and is known to comprise small donations from legitimate sources in the form of charitable donations, personal income or business revenue. Illegitimate sources of funds include fraud, criminal activities and money laundering whereas the methods of transfers differ from payment institutions to HAWALA, cash mules and cryptocurrencies, inter alia. Overall, the FATF (The Financial Action Task Force) Recommendations 2012-2023 identify customer due-diligence, record-keeping, and reporting suspicious activity as main preventive measures that help businesses combat money-laundering.

Furthermore, the FATF produced strategic guidance on the AML/ CFT risk-based approach for online casinos where it highlights the vulnerability of online casinos, and gaming sector as regards money laundering (ML) and terrorist financing (TF) risks ( page 59, Vulnerabilities of Casinos and Gaming Sector- March 2009) due to the key industry threats associated with the ever evolving techniques of online gambling fraud within the context of limited AML/CFT controls or regulatory responses in many jurisdictions.

From the payment methods standpoint, the volume of remote gambling transactions taking place over the online platforms with 24/7 accessibility is so large and the payment methods are so varied, that it is of paramount importance to develop efficient internal controls based on the periodic reviews of the results of the internal AML/CFT risk-assessments. Notably, the 2022 Supranational Risk Assessment Report by the European Commission identified the “gambling sector” and online gambling, as a “high risk” area of AML/CFT concern due to “the non-face-to face element, huge and complex volumes of transactions and financial flows” involving cryptocurrencies among other payment instruments. Prepaid cards have been identified as a highly popular method to acquire materials for the terrorist attacks and therefore it is important to conduct staff training based on newly available information.

The non-exhaustive list of conduct that may be indicative of terrorist financing risk include the following examples:

The parties to a transaction are based in a country or countries that are on a list of state sponsors of terrorism or a sanctions list.

Adverse media/ negative news screening reports indicative of links to the terrorist organizations.

Small regular deposits that are structured to avoid detection.

### **3.3. Proliferation Financing**

Nexus International Entertainment N.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, Nexus International Entertainment N.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, Nexus International Entertainment N.V. underscores its commitment to global non-proliferation efforts while maintaining the integrity and security of its operations.

### **3.4. Risk-based Approach**

A cornerstone of Nexus International Entertainment N.V. risk-based approach (RBA) is the execution of a thorough and ongoing risk assessment process. This process involves systematically evaluating risks across multiple dimensions, including customer profiles, products, services, and geographic locations. These assessments are conducted regularly to ensure potential vulnerabilities are identified and mitigated effectively, in alignment with both regulatory requirements and best practices.

#### Key Risk Factors Assessed

##### Customer Risk:

Nexus International Entertainment N.V. adopts a risk-based approach to compliance, placing strong emphasis on evaluating the potential exposure to money laundering (ML) and terrorist financing (TF) arising from its clientele. Each customer's profile—including their transaction behavior, sources of income, and financial background—is carefully assessed to identify any vulnerabilities that could pose a compliance risk.

Certain customer profiles inherently present higher risks. For example, individuals with multiple or opaque income sources may complicate the process of verifying the legitimacy of their funds. Similarly, clients who demonstrate unpredictable financial behavior or sudden shifts in spending patterns may raise red flags. Politically Exposed Persons (PEPs) are subject to enhanced scrutiny due to the increased corruption risks associated with their public functions and access to government-linked assets.

Additional indicators of higher-risk behavior include customers whose spending habits are inconsistent with their reported income, or those who operate multiple player accounts, potentially to obscure financial activity or bypass monitoring. To address such risks, Nexus International Entertainment N.V. sets transactional benchmarks aligned with normative customer behavior, enabling more efficient detection of anomalies.

By contrast, customers with a single, documented income stream and a stable financial history are generally regarded as low-risk. Individuals falling outside of this profile—those with complex financial arrangements or irregular transaction behavior—are flagged for closer monitoring and may be subject to Enhanced Due Diligence (EDD) protocols.

#### Product and Service Risk:

Products and services are analyzed to identify features that may increase risk, such as those facilitating high transaction volumes or allowing anonymous participation. Products with a higher likelihood of exploitation by criminal actors are subject to enhanced monitoring and control measures.

Not all gaming services or financial products carry the same level of risk. Some are more susceptible to abuse by criminal elements aiming to disguise or launder illicit proceeds. Nexus International Entertainment N.V. remains alert to the misuse of gaming platforms as a vehicle for financial crime.

Funds obtained through illegal activity—including fraud, trafficking, or theft—are often laundered through gambling ecosystems to mask their origin. Particular concern arises with the use of anonymous or semi-anonymous instruments such as prepaid cards, digital currencies, and gaming tokens, which present substantial traceability challenges.

Other concerning behaviors include the use of gaming accounts solely for storing or moving funds, as well as peer-to-peer transfers between players, which can be manipulated to conceal illegal financial flows. Additionally, the use of third-party financial tools—such as cards or accounts registered to individuals other than the account holder—adds further complexity to the audit trail.

Further risks emerge from ancillary financial services tied to the gaming environment, such as internal currency exchanges, credit services, and cross-platform functionalities, all of which are potential vectors for abuse. In response, Nexus International Entertainment N.V. employs robust monitoring tools, initiates EDD when warranted, and ensures full alignment with international anti-money laundering, counter-terrorist financing, and counter-proliferation financing (AML/CTF/CPF) standards.

#### Geographic Risk:

The company carefully assesses risks associated with the geographic regions of its customers and operations. Particular focus is placed on jurisdictions known for inadequate AML/CTF/CPF frameworks, high levels of corruption, or significant exposure to terrorism financing risks.

The geographical location of a customer and the origin of their funds are critical risk indicators. Jurisdictions known for inadequate AML/CTF governance, high corruption levels, or active sanctions programs are viewed as carrying elevated exposure to ML, TF, and CPF threats. Countries linked to terrorism or weapons proliferation are scrutinized with particular caution.

To evaluate these risks, Nexus International Entertainment N.V relies on authoritative international and regulatory sources, including but not limited to:

- FATF (Financial Action Task Force) watchlists identifying high-risk or monitored jurisdictions
- Public advisories from the Caribbean Financial Action Task Force (CFATF)
- The U.S. Department of State's INCSR (International Narcotics Control Strategy Reports)
- The European Commission's list of high-risk third countries with strategic AML/CFT deficiencies
- OFAC (Office of Foreign Assets Control) sanctions lists

#### Technological developments risk assessment

Nexus International Entertainment N.V maintains appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It identifies and assess the money laundering and terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

In those cases, a risk assessment takes place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism.

#### Mitigation Measures

Once risks are identified, Nexus International Entertainment N.V implements a series of tailored risk mitigation measures designed to address the specific risk level:

## Applying Targeted Risk Mitigation Measures

Once potential risks are identified, Nexus International Entertainment N.V. acts promptly to implement tailored mitigation strategies. These may include:

- **Reinforced Security Infrastructure**  
Introduction of strong identity verification processes, including multi-factor authentication (MFA), biometric verification, encrypted communications, and AI-based fraud detection systems to protect digital assets and user data.
- **Enhanced Monitoring Systems**  
Upgrading of transaction monitoring technologies to identify suspicious behavior patterns in real time. Automated tools are used to flag activities that deviate from expected financial behavior or suggest ML/TF intent.
- **Dynamic Policy Updates**  
Adaptation of the company's AML/CTF framework to reflect emerging technological threats. Nexus International Entertainment N.V. ensures that its policies evolve in parallel with advancements in financial crime techniques and cyber-enabled threats.

Through continuous evaluation and enhancement of its technological safeguards, Nexus International Entertainment N.V. reinforces its commitment to maintaining a secure, transparent, and fully compliant operational landscape. This proactive approach not only mitigates risks but also ensures that innovation is implemented responsibly—without compromising the company's regulatory obligations or exposing its financial ecosystem to criminal exploitation.

### Enhanced Due Diligence (EDD):

EDD is conducted for high-risk customers and transactions. This involves collecting additional information, such as the source of funds, beneficial ownership structures, and the purpose of the transactions. These measures provide deeper insights into customer profiles and transactional activities.

### Sophisticated Transaction Monitoring:

The company employs advanced transaction monitoring systems capable of setting alert thresholds and detecting suspicious patterns that may indicate ML, TF, or PF activities. These systems analyze transaction data in real time, flagging anomalies for further investigation.

### Robust Identity Verification:

For high-risk individuals, Nexus International Entertainment B.V. enforces rigorous identity verification protocols. These include checks through reliable sources,

cross-referencing data against sanctions lists, and ongoing monitoring to ensure customer profiles remain accurate and up-to-date.

### Ongoing Monitoring and Policy Adaptation

The company recognizes that continuous monitoring and periodic reviews are essential to maintaining an effective risk-based approach. Transaction data is regularly examined to identify suspicious activities, and customer profiles are updated as new information becomes available. AML/CTF/CPF policies and procedures are reviewed and revised periodically to ensure alignment with evolving risks, regulatory developments, and global best practices.

### Reporting and Record-Keeping

Accurate reporting and diligent record-keeping are integral to Nexus International Entertainment N.V. compliance framework. All suspicious transactions are promptly reported to the relevant authorities, ensuring regulatory obligations are met without delay. The company maintains comprehensive records of customer identification, transactional data, and risk assessments for the legally mandated retention period. These records are stored securely and made accessible for regulatory inspections when required, demonstrating Nexus International Entertainment N.V. commitment to transparency and accountability.

### Compliance with Curaçao's New Legislation

Nexus International Entertainment N.V. adheres to the updated requirements of the National Ordinance on Games of Chance (LOK), ensuring full compliance with Curaçao's revised AML/CTF/CPF framework. The company has established and implemented robust Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) programs, carefully tailored to align with its size, operational scope, and organizational complexity. These programs are grounded in a risk-based approach (RBA), which allows the company to allocate resources efficiently and prioritize high-risk areas to mitigate vulnerabilities effectively.

A critical component of this compliance strategy is comprehensive training for all employees. Regular and targeted training sessions are conducted to ensure staff members fully understand their responsibilities under the AML/CTF/CPF framework, with a specific focus on the principles of the RBA and effective risk management practices. This training equips employees to identify and address potential threats, ensuring they remain vigilant and capable of fulfilling regulatory obligations.

To maintain transparency and accountability, Nexus International Entertainment N.V. engages independent auditors to evaluate the effectiveness of its AML/CTF/CPF

programs. These audits assess the implementation of the RBA, the adequacy of internal controls, and the overall compliance of the company's policies and procedures with Curaçao's legislation. The insights gained from these audits are used to strengthen existing frameworks and ensure the company remains aligned with evolving regulatory standards.

Through these measures, Nexus International Entertainment N.V demonstrates its unwavering commitment to upholding Curaçao's new legislative requirements while ensuring the integrity and security of its operations.

#### Sector-Specific Risks in iGaming

In the gambling industry, Nexus International Entertainment N.V recognizes and addresses several sector-specific risks related to money laundering (ML), terrorist financing (TF), and proliferation financing (PF). The company has implemented tailored measures to manage these risks effectively, ensuring compliance with Curaçao's updated regulatory framework and maintaining the integrity of its operations.

#### Distribution Channel Risk

The types of channels used to establish business relationships can pose unique risks. Non-face-to-face interactions and anonymous channels increase exposure to fraud and identity theft, while reliance on unregulated third-party intermediaries can undermine AML/CTF/CPF controls. Nexus International Entertainment N.V. mitigates these risks through:

- Using advanced digital tools to verify customer identities and detect impersonation attempts.
- Ensuring that no anonymous or unregulated third parties are involved in client interactions.
- Strengthening controls around third-party service providers to confirm their compliance with AML/CTF/CPF regulations.

## **4. Customer Due Diligence**

Nexus International Entertainment N.V strictly complies with regulatory requirements prohibiting the creation or use of anonymous or fraudulent accounts. Verifying the identities of all players is a fundamental process in combating money laundering (ML), terrorism financing (TF), and proliferation financing (PF). The company ensures thorough identity verification procedures are in place, enabling a clear understanding of customer profiles and business relationships. This process not only

mitigates financial crime risks but also strengthens the integrity and transparency of its operations.

A robust Customer Due Diligence (CDD) program lies at the core of the company's risk management strategy. Through this program, Nexus International Entertainment N.V assesses customer risks and ensures adherence to legal and behavioral compliance standards. Enhanced due diligence (EDD) measures are applied to high-risk individuals or transactions, ensuring comprehensive risk assessment and monitoring.

If suspicious activities are identified, Nexus International Entertainment N.V promptly reports them to the Financial Intelligence Unit (FIU) of Curaçao in accordance with regulatory requirements. In cases where the severity of the activity necessitates further legal action, reports are escalated to the Public Prosecutor's Office. By taking these measures, Nexus International Entertainment N.V demonstrates its commitment to maintaining a secure and compliant gaming environment, aligned with Curaçao's updated regulatory framework.

#### **4.1. CDD Measures**

Nexus International Entertainment N.V enforces Customer Due Diligence (CDD) measures in a range of scenarios to ensure compliance with Curaçao's regulatory framework and to mitigate risks related to money laundering (ML) and terrorism financing (TF). CDD measures are implemented under the following circumstances:

Transactions Equal to or Exceeding NAF 4,000:

For any transaction involving an amount of NAF 4,000 or more, whether conducted as a single event or a series of linked transactions, CDD is mandatory.

Occasional Transactions Above NAF 4,000:

Occasional transactions that exceed this threshold, even if the customer does not maintain an ongoing relationship with the company, trigger the need for CDD measures.

Suspicion of Money Laundering or Terrorism Financing:

If there is any suspicion that a transaction may be connected to money laundering, terrorism financing, or proliferation financing activities, CDD measures are applied regardless of the transaction amount.

Uncertainties in Customer Identification:

When there are doubts or discrepancies in previously obtained customer identification information, Nexus International Entertainment N.V requires a fresh application of CDD to ensure accuracy and compliance.

### Linked Transactions Exceeding NAF 4,000:

Even if individual transactions fall below the NAF 4,000 threshold, the company assesses whether multiple linked transactions cumulatively exceed this amount. If so, these transactions are subject to CDD measures to prevent structuring or other illicit activities designed to evade detection.

### High-Risk Transactions:

Transactions flagged as high-risk due to customer profile, geographic origin, or other factors undergo Enhanced Due Diligence (EDD). This includes additional scrutiny of the source of funds, beneficial ownership, and the purpose of the transaction.

By applying these measures, Nexus International Entertainment N.V. ensures a robust framework for identifying and managing risks associated with financial crimes, safeguarding the integrity of its operations, and maintaining compliance with Curaçao's regulatory standards.

### Details of CDD Measures

Nexus International Entertainment N.V implements comprehensive Customer Due Diligence (CDD) measures as a critical component of its compliance framework. These measures ensure the accurate identification and verification of players, promote transparency, and reduce exposure to risks associated with money laundering (ML), terrorism financing (TF), and proliferation financing (PF). The company's approach to CDD includes the following key components:

#### Identifying and Verifying Players

##### Identity Verification:

Nexus International Entertainment N.V verifies the identities of all players using legitimate, reliable, and independent documents, data, or systems. Accepted documentation includes government-issued identification, passports, or other credible proof of identity, supplemented by technology-driven verification tools where applicable.

Identification Process: To establish a player's identity, the following details are collected:

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

In lower-risk scenarios, only basic details are needed. For higher-risk situations, more comprehensive information is collected to mitigate risks of money laundering and terrorism financing.

**Risk Assessment:** Initial risk ratings are assigned based on collected information and revised as more data is available. This helps determine the appropriate level of CDD.

**Verification Process:** Verification ensures that a player is who they claim to be through:

- Government-issued photo ID (e.g., passport, ID card)
- Supplementary documents (e.g., utility bill, bank statement) confirming address, no older than six months
- Verification of address through letters, email, or phone
- Biometric checks, cross-referencing database information, IP addresses, and funding methods

If the information collected is insufficient, additional steps may be taken, such as requesting a selfie with the ID or verifying the first deposit through a regulated financial institution.

#### Beneficial Ownership for Legal Entities:

For players acting on behalf of legal entities, the company identifies and verifies the ultimate beneficial owner (UBO). This includes analyzing the ownership and control structure to ensure clarity regarding who ultimately controls the entity. At the minimum identification information, verification and evidence are gathered for all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer. Where no natural person is identified under the 3 items mentioned above, the natural person who holds the position of senior managing official is being identified.

#### Purpose and Nature of Business Relationship:

A thorough understanding of the player's purpose for engaging with the casino and the nature of the business relationship is established. This helps the company assess whether the activities align with legitimate and expected behavior.

The company identifies the purpose and nature of its relationships with players as part of its CDD process. While the nature of the relationship might be clear, sufficient information is gathered to detect any unusual or suspicious activities. For higher-risk clients, detailed documentation of the source of wealth and expected activity levels is collected to ensure legitimacy. For lower and medium-risk players, a declaration with basic employment or business details suffices, while independent sources are used for higher-risk clients

### Ongoing Due Diligence:

Nexus International Entertainment N.V conducts continuous monitoring of player activity and transactions. This ensures consistency with the casino's knowledge of the player, their risk profile, and declared sources of funds. If necessary, enhanced scrutiny is applied to verify the origin of funds, particularly in high-risk scenarios.

Nexus International Entertainment N.V applies Customer Due Diligence (CDD) not as a one-time obligation, but as a continuous process throughout the entire customer relationship lifecycle. By embedding periodic reviews and dynamic risk evaluations into its broader compliance framework, the company ensures sustained alignment with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) requirements. This practice forms part of Nexus International Entertainment N.V overarching risk-based strategy, which is designed to adapt to emerging risks and maintain the integrity of its operations.

CDD procedures are actively applied to both new and existing customers. Central to this approach is the ongoing monitoring of transactions and the periodic reassessment of client risk profiles to ensure that the customer's activity remains within acceptable parameters.

#### Tailored Risk-Based Measures

For customers who were initially onboarded with incomplete or minimal due diligence, Nexus International Entertainment N.V conducts retrospective reviews. This includes:

- Re-evaluating and updating records for customers identified as having elevated risk;
- Scheduling routine updates to ensure that all stored data reflects the latest regulatory requirements and customer status.

#### When Re-Verification is Required

Nexus International Entertainment N.V re-applies full CDD measures in any of the following circumstances:

- A significant shift in the customer's behavior or profile, such as initiating unusually large or complex transactions, moving into a high-risk jurisdiction, or being reclassified as a Politically Exposed Person (PEP);
- Regulatory or legal updates requiring refreshed or additional customer information;

- When a pre-existing customer initiates a transaction or series of transactions that meet or exceed the company's defined threshold of NAF 4,000, thereby activating the full CDD requirement under the firm's AML policy.

### Remediating Gaps in Historical Due Diligence

In cases where clients were initially onboarded without full CDD being completed—often due to historical onboarding practices—Nexus International Entertainment N.V. undertakes corrective action as follows:

- Customers classified as high-risk are given priority for immediate identity and risk reassessment;
- Full CDD is applied systematically at intervals based on the specific risk rating assigned to the customer.

By ensuring that customer profiles are consistently reviewed and verified over time, Nexus International Entertainment N.V. strengthens its AML/CTF/CPF compliance posture, mitigates exposure to financial crime, and maintains a secure and transparent environment within its gaming operations

### Confidentiality of Reporting

The company takes confidentiality seriously when handling reports of suspicious activities

### No Tipping Off Players:

Staff members are strictly prohibited from informing players when a report has been submitted to the Financial Intelligence Unit (FIU). Maintaining discretion is essential to avoid tipping off individuals who may be involved in money laundering or terrorism financing activities.

### Bypassing CDD in Suspicious Cases:

In instances where completing the CDD process could alert the player to suspicions of illicit activity, Nexus International Entertainment N.V. bypasses the standard process. Instead, the company files a Suspicious Activity Report (SAR) directly with the FIU to ensure prompt and confidential reporting while avoiding any compromise to ongoing investigations.

By enforcing these detailed CDD measures, Nexus International Entertainment N.V. ensures compliance with Curaçao's AML/CTF/CPF regulatory framework. The company's efforts contribute to the prevention of financial crimes, safeguard the integrity of its operations, and uphold its commitment to regulatory compliance and ethical business practices.

## 4.2. Identification and Verification

Nexus International Entertainment N.V is committed to implementing a comprehensive and thorough process for identifying and verifying its players, ensuring compliance with Curaçao's regulatory framework and maintaining the integrity of its operations. This detailed approach to player identification not only minimizes the risks associated with money laundering (ML) and terrorism financing (TF) but also promotes a secure and trustworthy gaming environment. The identification and verification processes are designed to gather essential information, assess associated risks, and authenticate player identities through multiple layers of verification.

### Identification Process

To establish the identity of each player, Nexus International Entertainment N.V collects a wide range of information to ensure that individuals are accurately identified. The required information includes the player's full name, permanent residential address, date and place of birth, nationality, and a valid identity number. These details are fundamental to building a profile that accurately reflects the player's identity and serves as the foundation for further due diligence.

In cases where players are deemed to pose a lower risk, the company may limit the scope of information collection to these basic details. However, in higher-risk scenarios, where the likelihood of money laundering or terrorism financing is elevated, additional data is collected to mitigate potential risks. By tailoring the information requirements to the level of risk, the company ensures that its customer due diligence (CDD) measures are both proportionate and effective in addressing potential vulnerabilities.

### Risk Assessment

The initial risk assessment begins as soon as the player's information is collected, with a preliminary risk rating assigned based on various factors such as the player's geographic location, transaction patterns, and financial profile. This risk rating helps the company determine the appropriate level of scrutiny required for the player, ranging from standard CDD to Enhanced Due Diligence (EDD) in higher-risk situations. As the relationship with the player progresses and more data becomes available, the risk rating is continuously refined, ensuring that the company's monitoring processes remain dynamic and responsive to any changes in the player's behavior or circumstances.

This ongoing assessment allows Nexus International Entertainment N.V. to implement risk-based measures that align with the player's profile, ensuring that higher-risk customers are subject to stricter controls while lower-risk customers are managed with proportionate oversight.

#### Verification Process

The verification process is an essential component of the company's risk management strategy, ensuring that players are who they claim to be and that their activities are legitimate. This multi-layered process involves a combination of primary identification methods, supplementary documentation, and advanced verification tools to authenticate the player's identity with precision.

#### Primary Documents:

To verify a player's identity, Nexus International Entertainment N.V. requires the submission of a government-issued photo ID, such as a valid passport, national ID card, or driver's license. These documents serve as the primary evidence of the player's identity and are carefully reviewed for authenticity and validity.

#### Supplementary Documents:

In addition to primary identification, players are required to provide supporting documents to confirm their residential address. Acceptable documents include utility bills, bank statements, or similar records issued within the past six months. These supplementary documents help the company establish a verified connection between the player and their declared address.

#### Address Verification:

To further ensure accuracy, the company may use additional methods to confirm the player's residential address. This may involve sending correspondence to the address, verifying it through email or phone communication, or using third-party verification systems to validate the information provided.

#### Advanced Verification Tools:

Nexus International Entertainment N.V. leverages modern technological tools and techniques to enhance the verification process. This includes biometric checks such as facial recognition technology, cross-referencing player information against trusted databases, analyzing IP addresses to detect geographic inconsistencies, and assessing funding methods to ensure they align with the player's declared financial sources. These advanced tools provide an additional layer of security, helping to identify and address potential discrepancies in the player's profile.

#### Additional Measures for Insufficient Information

When the information provided by a player is insufficient or raises concerns about its accuracy or legitimacy, Nexus International Entertainment N.V takes additional steps to verify the player's identity. For instance, the company may request a selfie of the player holding their government-issued ID to confirm the document's authenticity and ensure the player's identity matches the provided information. In some cases, the company may also require the player to verify their first deposit through a regulated financial institution, further validating the legitimacy of their funding source and financial activities.

These measures are particularly important in high-risk situations, where the potential for money laundering or terrorism financing is greater. By taking these extra precautions, Nexus International Entertainment N.V ensures that even the most complex cases are handled with the utmost diligence and scrutiny.

#### Commitment to Compliance

Through its comprehensive player identification and verification processes, Nexus International Entertainment N.V upholds its commitment to regulatory compliance and the prevention of financial crimes. By collecting and verifying detailed player information, continuously assessing risk levels, and employing advanced verification tools, the company ensures that its operations remain secure and compliant with Curaçao's AML/CTF/CPF framework. These measures not only protect the company from potential risks but also contribute to the integrity and trustworthiness of the broader gaming industry.

### **4.3. Establishing and Understanding Relationships**

As part of its Customer Due Diligence (CDD) process, Nexus International Entertainment N.V ensures a thorough understanding of the purpose and nature of its relationships with players. While the nature of the relationship in the gaming sector is typically straightforward, the company collects sufficient information to identify and assess any unusual or suspicious activities that may arise during the course of the relationship.

For players categorized as higher-risk, Nexus International Entertainment N.V. takes additional precautions by gathering comprehensive documentation about their source of wealth, expected levels of activity, and any other relevant financial details. This in-depth approach ensures that the legitimacy of their funds and gaming activities is verified and that the company maintains compliance with AML/CTF/CPF regulatory standards.

In contrast, for players with a lower or medium-risk profile, the company employs a more streamlined approach. A basic declaration providing details of employment, occupation, or business activities is typically sufficient to establish the legitimacy of their relationship with the company. However, for higher-risk players, Nexus International Entertainment N.V. relies on independent and credible sources to validate the information provided, ensuring a greater degree of scrutiny and accuracy in such cases.

This tiered approach allows Nexus International Entertainment N.V. to tailor its due diligence measures to the specific risk level of each player, balancing efficiency with the need for robust compliance measures to detect and prevent potential financial crimes.

#### **4.4. Ongoing Monitoring**

Nexus International Entertainment N.V. places significant emphasis on the continuous monitoring of player identities and transactions as a critical component of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) policy. Ongoing monitoring ensures that the company remains vigilant against evolving risks and aligns its operations with regulatory requirements.

The company's monitoring process includes:

##### Regular Updates and Verification:

Player details are periodically reviewed and updated, with particular focus on high-risk individuals. This ensures that all information remains current and accurate, allowing for more effective risk assessments and compliance oversight.

##### Transaction Scrutiny:

Transactions are closely examined for unusual or suspicious patterns that may indicate potential money laundering, terrorism financing, or other illicit activities. This includes analyzing the frequency, volume, and geographic origin of transactions to detect anomalies.

##### Enhanced Due Diligence (EDD):

For transactions involving amounts of NAF 4,000 or more, including single transactions or multiple linked transactions that cumulatively exceed this threshold, the company applies Enhanced Due Diligence measures. This involves additional scrutiny of the source of funds, purpose of the transaction, and the legitimacy of the player's activities.

### Real-Time Monitoring Systems:

Nexus International Entertainment N.V. employs advanced transaction monitoring systems to identify potential red flags in real-time. These systems are designed to detect suspicious patterns and anomalies, enabling the company to act promptly by investigating the activity and, if necessary, reporting the findings to the Financial Intelligence Unit (FIU) of Curaçao.

By integrating these monitoring measures into its operational framework, Nexus International Entertainment N.V. ensures that it proactively identifies and mitigates risks, maintains compliance with Curaçao's AML/CTF/CPF regulations, and upholds the integrity of its gaming platform.

## 4.5. Enhanced Due Diligence, Simplified Due Diligence and PEP's

### Enhanced Due Diligence (EDD)

In high-risk scenarios, Nexus International Entertainment N.V. implements Enhanced Due Diligence (EDD) measures to ensure comprehensive scrutiny and mitigate potential risks associated with money laundering (ML), terrorism financing (TF), or proliferation financing (PF). These measures are designed to address the elevated risks posed by certain players, transactions, or circumstances. Key EDD procedures include:

#### Comprehensive Background Investigations:

A detailed examination of the player's background is conducted to assess their financial and personal profile. This includes verifying their professional history, financial activity, and any connections to higher-risk entities or jurisdictions.

#### Verification of Source of Funds and Wealth:

Nexus International Entertainment N.V. requires players to provide evidence of the source of their funds and overall wealth. This step ensures that the money used in transactions originates from legitimate and verifiable sources.

#### Close Analysis of Transaction Patterns:

Transaction activity is closely monitored to identify irregularities or suspicious patterns that may indicate potential financial crime. This includes evaluating the frequency, volume, and geographic origins of transactions.

#### Frequent Updates of Identification Information:

Identification details for high-risk players are updated regularly to ensure that all records remain accurate and up to date. This helps maintain the integrity of the company's compliance framework.

EDD measures are particularly stringent for Politically Exposed Persons (PEPs), as their elevated exposure to corruption risks necessitates thorough risk assessments and continuous monitoring. Ongoing scrutiny is applied to ensure that the player's activities remain consistent with the company's understanding of their risk profile.

All customer records are re-screened for PEP status at least annually and upon any significant account activity or profile update

### Simplified Due Diligence (SDD)

For low-risk scenarios, Nexus International Entertainment N.V applies Simplified Due Diligence (SDD) measures, which allow for a more streamlined approach to customer onboarding and monitoring. These measures are reserved for players or transactions that present minimal risk based on the company's risk assessment criteria. Key aspects of SDD include:

#### Basic Customer Information Collection:

Essential customer details, such as name, address, and basic identification, are collected without requiring extensive documentation or additional verification steps.

#### Less Frequent Reviews:

Player profiles and activities are reviewed at longer intervals compared to higher-risk scenarios, reflecting the reduced level of associated risk.

While SDD enables a more efficient process, Nexus International Entertainment N.V ensures that enhanced measures are promptly implemented if any suspicious activities are identified or if a player's risk profile changes. This flexibility ensures that the company maintains a balance between operational efficiency and regulatory compliance, safeguarding against potential threats at all risk levels.

### Handling Politically Exposed Persons (PEPs)

As part of its commitment to mitigating risks related to money laundering (ML), terrorism financing (TF), and proliferation financing (PF), Nexus International Entertainment N.V implements strict measures for handling Politically Exposed Persons (PEPs), their family members, and close associates. Recognizing that PEPs are inherently at higher risk of being involved in corruption or other financial crimes due to their positions of power, the company's AML/CTF/CPF policy mandates heightened scrutiny through Enhanced Due Diligence (EDD).

### The procedures for managing PEP-related risks include:

#### Obtaining Senior Management Approval:

Any decision to onboard or maintain a business relationship with a PEP requires prior approval from senior management. This ensures that the associated risks are thoroughly reviewed and endorsed at the highest level within the company.

#### Verification of Source of Funds and Wealth:

A comprehensive understanding of the PEP's financial background is required, including verifying the source of their funds and wealth. This step ensures that the player's financial activity is consistent with their declared profile and eliminates the risk of handling illicit or misappropriated assets.

#### Rigorous Ongoing Monitoring:

Nexus International Entertainment N.V. conducts continuous and detailed monitoring of PEP accounts and transactions to identify any unusual or suspicious patterns promptly. This includes assessing the volume, frequency, and nature of transactions against expected behaviors and maintaining updated profiles for the PEP and their associated entities.

#### Family Members and Close Associates:

The company extends its EDD measures to the family members and close associates of PEPs, as they may also present indirect risks by facilitating transactions or serving as intermediaries for illicit activities. These individuals are subject to the same level of scrutiny as the PEP themselves.

By implementing these measures, Nexus International Entertainment N.V. ensures that its operations remain compliant with Curaçao's regulatory requirements and international best practices. The company's proactive approach to handling PEPs reinforces its commitment to transparency, accountability, and the prevention of financial crimes.

## **4.6. Relationship Termination**

Nexus International Entertainment N.V. reserves the right to terminate its relationship with any player who engages in suspicious activities, fails to provide the required information, or otherwise poses an unacceptable level of risk. The decision to terminate a relationship is treated with the utmost seriousness, ensuring that appropriate steps are taken to comply with regulatory obligations and protect the integrity of the company's operations.

The termination process includes the following key steps:

Documentation and Approval:

Any decision to terminate a player relationship must be thoroughly documented, detailing the reasons for the termination and the associated risk factors. The decision is subject to review and approval by senior management, ensuring that it aligns with the company's AML/CTF/CPF policy and overall risk management strategy.

Comprehensive Review of Activities:

Upon termination, the player's activities are subjected to a detailed review. This includes an in-depth examination of all transactions conducted during the relationship to identify any patterns or activities that may warrant further investigation or reporting.

Reporting Suspicious Transactions:

If suspicious activities or transactions are identified during the termination process, they are promptly reported to the Financial Intelligence Unit (FIU) of Curaçao. This ensures compliance with regulatory requirements and supports broader efforts to combat financial crime.

Record Retention:

All records related to the terminated relationship, including identification documents, transaction histories, and termination-related documentation, are securely stored for a minimum of five years. This retention period ensures that the company can respond to any regulatory inquiries or audits that may arise in the future.

By enforcing a robust termination policy, Nexus International Entertainment N.V demonstrates its commitment to maintaining a secure and compliant gaming environment. This policy ensures that the company can effectively address potential risks while adhering to Curaçao's regulatory framework and international best practices.

## **4.7 CDD Timing**

Nexus International Entertainment N.V enforces Customer Due Diligence (CDD) measures swiftly and in alignment with established obligations under Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These measures are designed to ensure that all customer identities are accurately established and verified before significant financial interaction occurs.

### **Trigger Points for CDD Based on Transaction Activity**

Upon the creation of a player account, Nexus International Entertainment N.V. collects and verifies key identity details from each user, including:

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

As part of the company's risk-based compliance framework, identity verification is initiated prior to processing any financial transaction that meets or exceeds a threshold of NAF 4,000. This threshold is applied in the following scenarios:

- A single transaction equal to or above NAF 4,000
- A combination of transactions (such as multiple deposits, withdrawals, or internal transfers) that cumulatively reach this amount

Daily transaction data is monitored and aggregated per customer, enabling the company to identify when thresholds are met and respond in real time. Once the NAF 4,000 mark is reached, a full risk evaluation of the customer is conducted, and any remaining CDD steps are completed without delay.

#### Proactive CDD Measures at Onboarding

Nexus International Entertainment N.V emphasizes early completion of CDD. Identity checks are conducted at the point of registration, regardless of financial thresholds. This pre-emptive strategy is intended to prevent the entry of illicit funds into the system by ensuring that no user is granted full platform access without having first undergone due diligence.

#### Operational Limits for Incomplete CDD

- In situations where a player reaches the NAF 4,000 threshold prior to completing CDD, specific limitations are imposed:
- If triggered by a deposit: Further deposits and withdrawals are restricted; however, the customer may continue to participate in gaming using their current account balance.

If triggered by a withdrawal request: The player's account is temporarily frozen, and all gameplay is suspended until full verification is completed.

These safeguards help preserve the integrity of the platform and prevent unauthorized movement of funds during the verification window.

#### Consequences of CDD Non-Compliance

If a customer fails to submit the required documentation within 30 days after reaching the transaction threshold, the following measures are taken:

- The business relationship is terminated;
- If there are grounds for suspicion of ML or TF, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU);
- In the absence of suspicion, any remaining funds are returned to the source of deposit (e.g., the original bank account or digital wallet);
- Where suspicion persists, internal policies determine whether funds should be frozen pending further investigation, ensuring compliance with applicable law.

## 5. Suspicious Activity Reporting

Reporting suspicious activities in the gambling and betting industries is a critical component of maintaining the integrity of these sectors and preventing them from being exploited for illegal purposes such as money laundering, fraud, and corruption. Suspicious activity is reported for legal compliance purposes as failure to report can result in significant fines and legal consequences for individuals and businesses. It also helps ensure customer protection and helps safeguard customers from fraud and exploitation, ensuring a fair and safe environment for betting and gaming. Suspicious activity includes unusual transactions, structuring, unusual account activity and non-typical behavioral pattern, either too excessive or too disinterested in the betting outcomes, for instance. Unusual gambling patterns are investigated first to determine whether the exact nature of the transaction is just unusual or there are grounds to believe that it may be affiliated with the proceeds of a crime. According to article 1 of the Norut, it is an internet gambling entity's duty to report unusual transactions through the FIU Curacao's goAML portal which has been in use since January 1, 2021. Therefore, if the nominated officer determines that the internally reported suspicious activity should be disclosed to the regulatory authorities, he does so via the portal to comply with the Company's AML/CFT reporting protocol and obligations. In the meantime, the business relationship with the suspected customer is to be paused or terminated, depending on the circumstances.

Unusual transactions are those that deviate significantly from a customer's established financial behavior or profile. These might include unexpectedly high-value transactions, activity involving unknown third parties, or transfers that appear to serve no clear legal or economic function. Nexus International Entertainment N.V. leverages transaction monitoring systems to flag such anomalies, which are then forwarded to the Compliance Officer for detailed review.

Under the regulatory standards governing Nexus International Entertainment N.V, the following categories of transactions—whether completed or attempted—are considered potentially unusual and may require further investigation or formal reporting:

- **Previously Reported Suspicious Activity:**  
Any transaction that has already been submitted to law enforcement, such as the Police or the Department of Justice, for its suspected connection to money laundering (ML) or terrorist financing (TF) is classified as unusual by default.
- **Transactions Involving Sanctioned Parties:**  
Any transaction carried out by or on behalf of individuals, legal entities, or organizations listed under the *Sanctions National Ordinance (N.G. 2014 no. 55)*, or appearing on other official sanction lists, is deemed unusual.
- **Transactions at or Above NAF 5,000:**  
Regardless of the method—cash, electronic, check, or other payment formats—any transaction reaching this threshold is subject to enhanced scrutiny. Examples include:
  - Deposits or withdrawals of NAF 5,000 or more
  - Purchase of chips or credits in the same amount, including physical or digital equivalents
  - Payouts or redemptions that meet or exceed the threshold
- This applies not only to single transactions but also to series or combinations of smaller transactions that together total NAF 5,000 within a single day.
- **Transactions Suggesting ML or TF Activity:**  
If there are reasonable grounds to believe that a transaction may be linked to financial crime—based on contextual indicators or suspicious patterns—it must be treated as unusual and escalated accordingly.

#### Evaluation and Filing Procedures

When a report of an unusual transaction is received, the Compliance Officer reviews the information using internal risk parameters and regulatory standards. If the activity is deemed suspicious, a formal report is filed with the Financial Intelligence Unit (FIU) in compliance with Curaçao's AML framework. This decision is made after a comprehensive analysis to ensure it meets the legal threshold for suspicious activity.

Nexus International Entertainment N.V keeps detailed records of all transactions and activities that seem suspicious, including dates, amounts, methods, and any other relevant details. As regards customers, the anti-fraud and AML teams document all

available information about the individuals or entities involved, including names, addresses, account numbers, and identification.

## **6. Sanctions Compliance and Monitoring**

Nexus International Entertainment N.V is steadfast in its commitment to adhering to international sanctions and regulatory standards as part of its comprehensive Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) policy. The company implements rigorous procedures to ensure compliance with all sanctions imposed by national and international authorities, safeguarding its operations and mitigating financial crime risks.

### Thorough Due Diligence on Clients and Transactions

To meet these obligations, Nexus International Entertainment N.V conducts exhaustive due diligence on all clients and transactions. This process aims to prevent any direct or indirect interaction with individuals, entities, or regions listed under sanctions. The company diligently screens clients and their transactions to identify potential risks, ensuring that no activities breach applicable sanctions regulations.

### Ongoing Monitoring and Reporting

Monitoring and reporting play a central role in the company's sanctions compliance framework. Nexus International Entertainment N.V. employs advanced systems to continuously monitor all client transactions, ensuring they remain free from suspicious activities that could contravene sanctions laws.

Real-Time Monitoring: Automated systems are used to verify transactions and interactions against the most recent Sanctions Lists in real-time.

Prompt Reporting: Any anomalies or suspicious activities detected during monitoring are escalated immediately to the relevant authorities, such as the Financial Intelligence Unit (FIU), ensuring prompt resolution.

**Decisive Action:** In cases where a match or suspicious activity is identified, the company takes swift and decisive measures, including freezing accounts, blocking transactions, and conducting account reviews.

### Commitment to Staff Training and Awareness

The company reinforces its compliance culture through ongoing staff training programs designed to keep all personnel informed about current sanctions regulations and their implications. These training sessions cover the latest updates

to sanctions lists and best practices for detecting and reporting potential breaches. By maintaining a well-informed workforce, Nexus International Entertainment N.V. ensures that compliance efforts are consistently robust and effective.

### Regular Reviews and Updates

Nexus International Entertainment N.V recognizes the dynamic nature of sanctions legislation and ensures that its compliance framework is regularly reviewed and updated to align with evolving regulations. This includes maintaining up-to-date access to key sanctions lists, such as:

Sanctions National Ordinance (SNO, N.G. 2014, no. 55) and Kingdom Sanction Act (N.G. 2016, no. 54).

Curaçao Gaming Control Board (GCB) announcements.

European Union (EU) Sanctions.

United Nations Security Council Consolidated List.

UK Office of Financial Sanctions Implementation (OFSI) Sanctions.

US List of Foreign Terrorist Organizations and Office of Foreign Assets Control (OFAC) Sanctions.

The company's due diligence procedures are designed to uncover indirect or covert attempts to engage with sanctioned parties or jurisdictions. If any evasion tactics are discovered, they are promptly reported to the relevant authorities, and immediate corrective measures—such as transaction suspensions, account freezes, or intensified reviews—are implemented.

## **7. Senior Management**

Senior management at Nexus International Entertainment N.V plays a critical role in evaluating and managing risks related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF). By providing strategic oversight and leadership, senior management ensures that the company's policies, procedures, and control environment remain robust, effective, and aligned with both regulatory requirements and global best practices.

To facilitate effective oversight, the Board of Directors mandates that the appointed AML/CTF/CPF Officer provides regular updates on significant developments or issues within the company's control environment. In addition, the officer is required to submit an annual report assessing the effectiveness of the company's AML/CTF/CPF measures and controls. This report serves as a key tool for

evaluating the company's ability to mitigate risks associated with money laundering, terrorism financing, and proliferation financing.

### Annual Reviews and Risk Assessments

Senior management conducts comprehensive reviews of all relevant AML/CTF/CPF policies and procedures at least once a year. These reviews are guided by insights from monthly risk assessments, which help identify potential weaknesses or gaps in the company's internal controls and risk management framework.

In cases where deficiencies are identified, the AML/CTF/CPF Officer is empowered to recommend adjustments to the Board of Directors. These proposed changes are carefully reviewed and, upon approval, implemented to enhance the company's ability to manage risks and maintain regulatory compliance. By addressing these weaknesses proactively, Nexus International Entertainment N.V ensures that its internal controls remain resilient against evolving threats.

### Employee Training and Awareness

A critical component of senior management's role involves overseeing the development and execution of comprehensive employee training programs. These programs are designed to increase awareness and understanding of AML/CTF/CPF risks, ensuring that all employees, especially those in key roles, are well-equipped to detect and respond to suspicious activities. As part of our framework, we have established thorough policies and procedures for employee background screening and conduct regular training for all relevant personnel.

Training sessions are regularly updated to incorporate the latest regulatory requirements, industry best practices, and emerging trends in financial crime. This ensures that the company's workforce remains informed and capable of upholding the highest standards of compliance.

### Internal Control Framework

Senior management ensures that the company's internal control framework is robust and well-structured to support effective risk management. Key elements of this framework include:

- Segregation of Duties: Assigning distinct responsibilities to different personnel to minimize the risk of fraud or errors.
- Authorization Processes: Establishing clear and well-documented approval procedures for critical decisions and transactions.
- Ongoing Monitoring: Implementing systems and processes to continuously monitor activities, identify anomalies, and detect potential risks in real-time.

- **Thorough Documentation:** Maintaining detailed records of all transactions, decisions, and risk management activities to facilitate audits and regulatory reviews.

### Independent Audits and Assessments

To ensure the ongoing effectiveness of the AML/CTF/CPF program, senior management commissions regular independent audits and assessments. These evaluations provide an objective review of the company's compliance framework, highlighting strengths while identifying areas that require improvement. The findings from these audits are used to refine the company's policies and procedures, further reinforcing its commitment to regulatory compliance and effective risk management.

By maintaining active oversight, fostering a culture of compliance, and implementing robust internal controls, senior management at Nexus International Entertainment N.V ensures that the company remains well-prepared to address risks related to money laundering, terrorism financing, and proliferation financing. This proactive approach not only strengthens the company's defenses against financial crimes but also underscores its dedication to operating with integrity and transparency.

## **8. Compliance Function**

### Appointment and Role of the Compliance Officer

At Nexus International Entertainment N.V the appointment of a qualified individual as the Compliance Officer is a cornerstone of the company's Anti-Money Laundering (AML) strategy. This appointment, made by senior management, ensures the role's independence and authority, providing the necessary autonomy to oversee the effective implementation of AML policies and procedures. The Compliance Officer is a senior-level professional with substantial expertise in AML compliance and related regulatory frameworks. The position is formalized through an official appointment letter, which outlines their responsibilities, authority, and reporting structure within the organization.

### Primary Functions of the Compliance Officer

The Compliance Officer performs several critical functions to ensure the effectiveness and robustness of the company's AML program. These responsibilities include:

1. Policy Implementation:  
Overseeing the execution of AML policies and procedures and ensuring that

they remain fully aligned with Curaçao's regulations and international best practices.

2. Central Point of Contact:

Acting as the primary contact for all AML-related concerns, including internal queries from employees and external communications with regulatory authorities.

3. Policy Review and Updates:

Conducting regular reviews and updates of AML policies to reflect changes in regulations, emerging risks, and evolving financial crime trends.

4. Training Oversight:

Managing the company's AML training program to ensure that all employees, especially those in high-risk roles, are equipped with the knowledge and skills to identify and respond to suspicious activities effectively.

### Core Responsibilities of the Compliance Officer

The Compliance Officer is entrusted with several pivotal responsibilities that are essential for the ongoing success of the AML program:

1. Transaction Monitoring and Reporting:

- o Continuously monitoring client transactions and activities to identify unusual patterns or suspicious behavior.
- o Filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) of Curaçao as required.
- o Maintaining detailed and accurate records of all SARs and related documentation, ensuring these are available for regulatory review.

2. Policy Development and Updates:

- o Crafting, updating, and refining AML policies and procedures to comply with Curaçao's gaming regulations and international standards.
- o Adjusting the AML framework proactively to address new risks and regulatory developments.

3. Employee Training and Awareness:

- o Designing and delivering comprehensive AML training sessions to ensure employees understand their roles and responsibilities in detecting and reporting suspicious activities.

- o Updating training materials regularly to incorporate legislative changes, emerging trends, and feedback from regulatory audits or inspections.

#### 4. Regulatory Liaison:

- o Acting as the primary liaison with regulatory bodies, law enforcement agencies, and other relevant authorities on AML matters.
- o Responding promptly to information requests, inquiries, and participating in regulatory inspections or audits to demonstrate the company's compliance efforts.

#### 5. Compliance Audits and Corrective Actions:

- o Conducting regular internal audits to evaluate the effectiveness of the AML program and ensure adherence to all legal and regulatory requirements.
- o Addressing any identified deficiencies or gaps through corrective measures, ensuring continuous improvement of the company's compliance framework.

#### 6. Record-Keeping:

- o Maintaining comprehensive records of all AML-related activities, including SAR filings, internal reports, training sessions, and policy updates.
- o Ensuring these records meet legal retention requirements and are readily accessible for review by regulatory authorities.

### Importance of the Compliance Officer's Role

By fulfilling these functions and responsibilities, the Compliance Officer plays a pivotal role in protecting Nexus International Entertainment N.V from risks associated with money laundering, terrorism financing, and proliferation financing. This position is integral to maintaining the company's compliance with Curaçao's AML regulations and safeguarding its reputation in the gaming sector.

Through diligent policy implementation, effective risk management, and continuous engagement with employees and regulators, the Compliance Officer ensures that the company upholds the highest standards of integrity and regulatory compliance.

## **9. Audit Function**

## Independent Audit and Oversight for AML/CTF/CPF Compliance

In alignment with the updated gaming regulations in Curaçao, Nexus International Entertainment N.V. undergoes an independent audit focused on its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) practices. This audit process is a critical aspect of ensuring compliance with Curaçao's legal framework and maintaining the integrity of the company's operations.

This section outlines the comprehensive audit process, detailing the role of the independent auditor and the review conducted by the Curaçao Gaming Control Board (GCB).

### Purpose and Scope of the AML/CTF/CPF Audit

The primary objective of the annual AML/CTF/CPF audit is to evaluate the effectiveness and compliance of the company's policies, procedures, and controls. This audit helps Nexus International Entertainment N.V. adhere to current legal standards, mitigate risks associated with money laundering and terrorism financing, and align with global best practices.

The audit encompasses a detailed evaluation of the company's AML/CTF/CPF program, including the following key areas:

- **Risk Assessments:** Analyzing the accuracy and effectiveness of the company's risk assessments and corresponding mitigation strategies.
- **Transaction Monitoring Systems:** Assessing the efficiency of systems used to detect and report suspicious activities.
- **Staff Training Programs:** Evaluating the adequacy and impact of training initiatives to ensure employees understand and fulfill their AML/CTF/CPF responsibilities.
- **Reporting Mechanisms:** Reviewing procedures for filing Suspicious Activity Reports (SARs) and compliance-related issues.
- **KYC, KYB, and CDD Protocols:** Verifying adherence to Know Your Customer (KYC), Know Your Business (KYB), and Customer Due Diligence (CDD) requirements.

### Selection of the Independent Auditor

Nexus International Entertainment N.V. engages an independent auditor with substantial expertise in AML/CTF/CPF compliance. The chosen auditor may be an

external professional or an internal audit team independent of the company's AML Compliance department to avoid conflicts of interest.

When selecting an auditor, the company considers the individual or firm's credentials, experience, and reputation within the industry. Additionally, the Curaçao Gaming Control Board (GCB) must approve the selected auditor to ensure compliance with regulatory standards. This dual-layered approval process reinforces the credibility and objectivity of the audit.

#### Audit Process and Standards

The audit process adheres to international standards and specific requirements outlined by the GCB. The key elements of the audit include:

1. Evaluation of AML/CTF/CPF Policies and Procedures:  
Ensuring that the company's policies are up-to-date, compliant with legal requirements, and effectively implemented.
2. Risk Management Assessment:  
Reviewing the company's risk management framework to determine the effectiveness of its assessments and mitigation strategies.
3. Transaction Monitoring Review:  
Assessing the functionality and reliability of systems used to monitor transactions and identify suspicious patterns.
4. Staff Training Evaluation:  
Analyzing the scope, frequency, and quality of employee training programs to ensure employees are equipped to recognize and address financial crime risks.
5. Reporting Mechanism Audit:  
Examining the effectiveness of the company's procedures for reporting suspicious transactions and other compliance-related issues to the Financial Intelligence Unit (FIU).
6. Customer File Review:  
Verifying compliance with KYC, KYB, and CDD requirements by reviewing customer profiles, documentation, and transaction records.

#### Audit Reporting and Corrective Actions

Following the audit, the independent auditor produces a comprehensive report detailing findings, recommendations, and any identified issues. This report is presented to the company's senior management and submitted to the Gaming Control Board for review.

Nexus International Entertainment N.V. is committed to addressing the auditor's recommendations promptly. Corrective actions are implemented within a specified timeframe, and follow-up audits may be conducted to confirm that these measures have been applied effectively.

#### Oversight by the Gaming Control Board

The Gaming Control Board plays a pivotal role in overseeing AML/CTF/CPF compliance for all licensed operators, including Nexus International Entertainment N.V. The Board reviews audit results, conducts its own evaluations, and ensures that operators address identified deficiencies.

The Board's examination process includes:

1. **Audit Report Review:** Analyzing the independent auditor's report to assess compliance and identify concerns.
2. **Onsite Inspections:** Conducting visits to the company's premises to validate audit findings and evaluate the implementation of corrective actions.
3. **Interviews and Documentation Analysis:** Engaging with relevant staff members and reviewing documentation to gain a comprehensive understanding of the company's AML/CTF/CPF practices.

If non-compliance is identified during the audit or the Board's examinations, the company acknowledges that penalties may be imposed. These penalties could include fines, operational restrictions, or even suspension or revocation of the company's gaming license. Nexus International Entertainment N.V. is committed to working closely with the Gaming Control Board to resolve any issues, implement corrective measures, and maintain full compliance to prevent future violations.

Through rigorous independent audits, effective corrective actions, and close collaboration with the Gaming Control Board, Nexus International Entertainment N.V. ensures that its AML/CTF/CPF practices remain robust, compliant, and aligned with Curaçao's evolving regulatory landscape.

## 10. Employee Training Program

Nexus International Entertainment N.V. employees play a crucial role in Anti-Money Laundering (AML) compliance within the betting and gambling industries. Their actions and vigilance are essential in preventing these sectors from being exploited for money laundering and other illicit activities. They are made aware of the fact that

failing to report potential breaches of AML Policies may lead to administrative and criminal charges.

The Company's employees, especially those in customer-facing roles or positions that involve handling financial transactions, must have a thorough understanding of the company's AML policies and procedures. This includes knowing the types of transactions that should be considered suspicious, the process for reporting such transactions, and the importance of maintaining customer confidentiality.

A key part of an employee's role in AML compliance is to be vigilant and identify any activities that seem unusual or do not fit with the normal behavior of a customer. This could include large and inconsistent bets, frequent changes in betting patterns, or transactions that seem to have no apparent purpose other than to move money through the system.

Once an employee identifies a potentially suspicious transaction, they must report it through the appropriate channels to the Compliance Officer. The reporting protocol involves filling out a Suspicious Activity Report (SAR) and using the company's internal reporting system. Employees are trained on how to report suspicions and the importance of doing so promptly on an annual basis or more frequently in line with the needs of a particular department.

Employees involved in customer onboarding or account management are responsible for conducting due diligence checks on customers. This includes verifying their identity, understanding the source of their funds, and ensuring that they are not listed on any sanctions or watch lists. Employees are trained on how to conduct such checks diligently and escalate any concerns where necessary.

Employees involved in AML compliance at Nexus International Entertainment N.V. understand the importance of maintaining the confidentiality of their reports and any information related to suspicious activities. They are made aware of data protection laws and ensure that customer information is handled in compliance with these regulations.

## **11. Record - Keeping**

Nexus International Entertainment N.V. is subject to The Company complies with all the relevant legislation as regards having an audit trail in cases where it is asked to assist in the investigations by law enforcement agencies. Generated records are retained in electronic form for a period of 5 years in accordance with the data

protection regulations from the date of the establishment of a business, commercial or a professional relationship with an employee, a customer or a business partner.

Such a business relationship arises between the Company and a customer from the time when an account is open until the time when the relationship is terminated. During the relationship the Company undertakes to satisfy CDD measures stipulated in the legislation and carry out an ongoing monitoring of the account activity to adjust its risk rating where necessary.