

GEOSIX B.V. (163931)

License Number: OGL/2024/316/0598

**Policy for combating
Money Laundering, the Financing of
Terrorism and Proliferation of weapons of
Mass Destruction (ML/FT/FP)**

Approved by:

Geosix N.V Executive Board



Effective Date: 01st of February 2025

Responsible Compliance Officer:

Semen Klyuchyk

compliance@geosix.net

Contents

I.	Introduction.....	3
II.	iGaming Landscape.....	3
III.	Risk Assessment of ML & TF.....	10
IV.	Clients and players Due Diligence.....	15
V.	Sanctions.....	25
VI.	Suspicious Activity Reporting.....	26
VII.	Compliance Officer.....	27
VIII.	ML/FT/FP Audit.....	29
IX.	Employee screening program and training.....	30
X.	Record Keeping Procedure.....	32
XI.	Senior Management Obligations & Responsibilities.....	32
	Annex 1 – Definitions.....	33

The information contained herein is the property of Geosix B.V and its associated entities and may not be copied, used or disclosed in whole or in part outside of the group of companies without prior written permission.

Proprietary & Confidential

I. Introduction

Geosix B.V. is a legal entity registered in Curaçao under registration number 163931. The company owns and manages the website: <https://vippari.com/>

Geosix B.V. ("the Company", "we", "ours") operates under a Curaçao online gaming license issued by the Curaçao Gaming Control Board OGL/2024/316/0598, complying with the licensing requirements and regional restrictions set by the Curaçao regulatory authorities. These regulations prohibit their remote gaming licensees from offering services in the US, Australia, Dutch West Indies (Aruba, Bonaire), Curacao, France, Germany, the UK, Belize, and the Netherlands. The company operates only in markets where it is permitted and does not target customers in jurisdictions where online gambling is banned.

E-gaming and betting operators face money laundering risks, including identity theft and fraud, structuring, layering, and collusion between employees and customers or external payment providers to bypass internal safeguards.

II. iGaming Landscape

The Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction Policy (further referred to as ML/FT/FP Policy) was developed to comply, first and foremost, with the guidelines of the ML/FT/FP supervisor in Curaçao, the Curaçao Gaming Control Board. The company's directors, officers, and employees are committed to upholding the standards set forth in the Policy. This Policy applies to all company personnel, counterparties, and third-party consultants, inter alia.

Geosix B.V.'s Board of Directors (BoD) approves the framework for designing, implementing, and monitoring the ML/FT/FP Policy on an annual basis. Furthermore, the policy may also be updated periodically to reflect significant changes in ML/FT/FP regulations or operational practices. Additionally, a designated officer may propose urgent changes based on internal and third-party AML audit recommendations concerning risk probability and impact.

The ML/FT/FP Policy is designed to combat money laundering and the financing of terrorism, uphold the highest industry standards, and maintain compliance with both domestic and international ML/FT/FP regulatory frameworks. This policy establishes a unified, risk-based methodology that rigorously addresses threats associated with customers, products and services, payment systems, geographic regions, and distribution channels.

It is aligned with key global anti-money laundering and counter-terrorism financing objectives and complies with the prevailing legislative framework in Curaçao. This includes the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (PB 1993, no. 63) (NOOGH), the National Ordinance on the Penalization of Money Laundering (NOPML),

the National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017, no. 99) with amendments effective May 16, 2024, and the National Ordinance on Identification when Rendering Services (NOIS, N.G. 2017, no. 92) with its corresponding 2024 amendments. It also references the Sanctions National Ordinance (SNO, N.G. 2014, no. 55) and the Kingdom Sanctions Act (N.G. 2016, no. 54).

Furthermore, the policy integrates internationally recognized standards and frameworks such as the Financial Action Task Force (FATF) Recommendations, the 4th, 5th, and 6th European Union Anti-Money Laundering Directives (AMLDs), and the Wolfsberg Group Principles.

Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

Money laundering plays a critical role in financial crimes, often involving international transactions and operations. It is associated with a range of illegal activities, including tax fraud, corruption, sanctions evasion, drug trafficking, illicit arms trade, extortion, and kidnapping. The primary purpose of money laundering is to obscure the illegal origins of financial gains, making it difficult to trace their source, ownership, and ultimate destination.

Money Laundering

It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement – This initial phase involves introducing illegally obtained funds into the financial system. This can occur through bank deposits, acquiring high-value assets, or conducting various financial transactions. The objective at this stage is to begin integrating illicit proceeds into the legitimate economy.
- Layering – During this stage, funds are transferred through multiple transactions to create complexity and obscure their origins. This may involve moving money between multiple accounts, converting funds into different currencies, or investing in financial instruments. The intent is to make tracing the transactions back to their criminal source increasingly difficult.
- Integration – In the final phase, laundered funds are reintroduced into the legal economy. This may involve purchasing luxury assets, investing in cash-intensive businesses, or engaging in other seemingly lawful financial activities. At this stage, the illicit funds appear legitimate, making them harder to identify and track

Most of the people think that money laundering refers to funds acquired with drugs trafficking, but there are many predicate offences for money laundering such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes

Terrorist Financing and Its Link to Money Laundering

To mitigate such risks, **Geosix B.V.** ensures that employees receive continuous training on emerging trends and evolving threats associated with terrorist financing.

Risk Management and Compliance Measures

To proactively combat money laundering risks, **Geosix B.V.** has implemented comprehensive compliance measures to identify, assess, and mitigate potential threats. These include:

- Fraud Prevention and Identity Verification – Conducting customer due diligence (CDD) through document verification, age authentication, and location validation.
- Monitoring Multiple Accounts and High-Value Transactions – Identifying irregular account behavior, such as the use of multiple accounts or frequent large transactions.
- Detecting Suspicious Deposits – Screening for funds that may originate from illicit activities and ensuring the platform is not misused as a temporary holding space for such transactions.
- Player-to-Player Transfers – Monitoring transactions between users to detect potential misuse for laundering illicit funds or fraudulent cash-outs.

These measures represent key components of the company's AML compliance efforts; however, new risks may emerge over time. To ensure continued effectiveness, **Geosix B.V.** conducts regular risk assessments tailored to evolving threats and provides ongoing training to its employees. This reinforces the company's commitment to a robust Anti-Money Laundering (AML) compliance framework.

Terrorism Financing:

Terrorism financing involves the provision of financial support to terrorist organizations or activities, utilizing both lawful and unlawful financial sources. These funds are essential for carrying out operations, ranging from minor logistical support to large-scale attacks.

Sources of Terrorism Financing

The funding sources for terrorist activities can generally be categorized into two groups:

- Legitimate Sources – Terrorists often exploit legal financial systems, including businesses, charitable donations, and other lawful transactions, to redirect funds covertly. In some instances, charitable organizations and commercial enterprises are misused as intermediaries to conceal and reroute financial resources.
- Illicit Sources – Criminal activities such as fraud, smuggling, drug trafficking, extortion, and money laundering serve as primary means of generating funds while obscuring their origins.

Methods of Fund Transfers

Terrorist networks employ various channels to transfer and distribute funds, including:

- Formal Financial Institutions – Traditional banking systems and financial services are sometimes manipulated using advanced techniques such as layering and structuring. These methods involve breaking large transactions into smaller amounts to avoid raising suspicion and bypass financial monitoring mechanisms.
- Informal Money Transfer Systems – Alternative financial networks, such as the hawala system, operate outside conventional banking regulations, making it difficult for authorities to detect and trace suspicious transactions.

Indicators of Terrorism Financing

Certain financial behaviors and transaction patterns may signal potential terrorist financing, including:

- Unusual financial activities that deviate from an individual's or business's normal behavior.
- Frequent or high-value transactions linked to regions associated with terrorist activity.
- Financial dealings involving individuals or organizations flagged on international sanctions or watchlists.
- Large cash deposits, transactions involving high-risk industries, or activities designed to evade detection by financial institutions.

Financing of Proliferation of weapons

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials

Regulatory Compliance and Countermeasures

To mitigate the risks associated with terrorism financing, **Geosix B.V.** has established a robust Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) compliance framework, which includes:

- Customer Due Diligence (CDD) – Conducting thorough identity verification, assessing the source of funds, and evaluating potential risks.
- Transaction Monitoring – Continuously analyzing financial transactions to detect patterns indicative of suspicious activities.
- Reporting Suspicious Activities – Promptly notifying the relevant authorities whenever transactions raise red flags related to terrorism financing.

Furthermore, the company strictly adheres to various international and national regulatory frameworks, including:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- Curaçao Gaming Control Board (GCB) regulatory requirements
- Office of Foreign Assets Control (OFAC) sanctions and watchlists
- United Nations Security Council (UNSC) sanctions list
- European Union (EU) anti-terrorism financing regulations
- U.S. List of Foreign Terrorist Organizations

These regulatory measures ensure that **Geosix B.V.** does not inadvertently facilitate financial transactions that could support terrorist organizations

Global Counter-Terrorism Financing Initiatives

To align with international standards, **Geosix B.V.** complies with established counter-terrorism financing frameworks, including:

- Financial Action Task Force (FATF) – An international body that sets guidelines for detecting and preventing financial crimes related to terrorism and money laundering.
- Office of Foreign Assets Control (OFAC) – A U.S. government agency responsible for enforcing economic sanctions and maintaining the Specially Designated Nationals (SDN) list, which includes entities linked to terrorism.
- European Union (EU) Regulations – Mandating strict AML/CTF measures across member states to prevent financial exploitation by terrorist groups.
- United Nations (UN) Sanctions – Imposing global restrictions and maintaining watchlists of individuals and organizations associated with terrorism financing.

By implementing stringent compliance policies and adhering to international regulations, **Geosix B.V.** reinforces its ability to identify, prevent, and report terrorism financing activities, ensuring a secure and legally compliant operational environment.

Proliferation Financing:

Proliferation financing refers to the financial support, facilitation, or provision of resources for activities related to the development, acquisition, and distribution of weapons of mass destruction (WMDs) and their delivery systems. This form of financial crime poses a significant global security risk and is strictly prohibited under both international regulations and Curaçao's legal framework. As a licensed iGaming operator, **Geosix B.V.** (Reg. Number: 163931) is committed to identifying, assessing, and mitigating the risks associated with proliferation financing. This commitment is embedded within the company's broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework, ensuring full regulatory adherence and the integrity of its financial transactions.

Compliance with Curaçao iGaming Regulations

The Curaçao Gaming Control Board (GCB) enforces strict regulatory requirements to prevent financial crimes, including proliferation financing. These regulations require all licensed iGaming operators, including **Geosix B.V.** to take active measures in identifying, mitigating, and reporting potential threats linked to WMD proliferation. By complying with these regulations, the company aligns itself with global financial security standards, ensuring that its platform is not exploited for illicit financial activities.

Risk Assessment and Proliferation Financing Prevention

To effectively counter the risks associated with proliferation financing, **Geosix B.V.** conducts comprehensive risk assessments on an ongoing basis. These assessments focus on identifying customers and financial transactions that may be linked to high-risk jurisdictions known for weak proliferation controls. In particular, the company examines transactions involving goods, services, or entities associated with proliferation networks and evaluates financial patterns that resemble established proliferation financing methods. By continuously refining its risk assessment strategies, the company enhances its ability to detect and prevent any attempts to misuse its platform for illicit financial purposes.

Geosix B.V. shall conduct a Business Risk Assessment (BRA) and a Customer Risk Assessment (CRA). The BRA will evaluate risks related to VIP programs, and online gaming platforms. Each player will be assigned a risk category (low, medium, or high) based on a CRA conducted during onboarding. These assessments shall be reviewed at least annually or whenever significant changes in operations occur, such as the launch of new products.

Enhanced Customer Due Diligence (CDD) Measures

As part of its stringent compliance framework, **Geosix B.V.** implements enhanced customer due diligence (CDD) procedures, particularly for customers and transactions categorized as high-risk. These procedures include screening all customers against international sanctions lists, including those maintained by the United Nations Security Council (UNSC), the Financial Action Task Force (FATF), and the European Union (EU). Additionally, the company thoroughly investigates any transactions that deviate from typical customer behavior and closely monitors potential affiliations with organizations flagged for involvement in proliferation-related activities. These proactive measures ensure that the company effectively identifies and prevents high-risk transactions from occurring within its platform.

Transaction Monitoring and Suspicious Activity Reporting

To detect financial activities that may be linked to proliferation financing, Company's employs sophisticated transaction monitoring systems designed to analyze patterns of financial behavior. These systems continuously scan financial transactions, flagging any movements that exhibit characteristics of proliferation financing. When suspicious activity is identified, it is immediately reviewed by compliance officers, who conduct further investigations before submitting Suspicious Activity Reports (SARs) to the

Curaçao Financial Intelligence Unit (FIU) via the goAML online portal. Compliance staff will maintain complete records of reports and supporting evidence and shall ensure timely submission in accordance with regulatory requirements. This ensures that regulatory authorities are promptly informed of any potential proliferation financing risks, enabling swift enforcement actions against any entities attempting to exploit the financial system.

Sanctions Screening and Regulatory Compliance

Strict adherence to Curaçao and international sanctions regulations is a core component of **Geosix B.V** compliance program. The company systematically screens all financial transactions and business relationships against regularly updated sanctions lists, including those under the Kingdom Sanction Act and United Nations Security Council Resolutions. Transactions involving individuals, entities, or jurisdictions subject to WMD-related sanctions are automatically flagged and blocked, preventing illicit financial flows from infiltrating the platform. Additionally, the company maintains detailed records of all sanction's screenings and compliance actions, ensuring full transparency and accountability during regulatory audits.

Training and Awareness for Employees

Recognizing the importance of informed decision-making in preventing proliferation financing, **Geosix B.V** ensures that all employees receive specialized training on financial crime risks, with a particular focus on proliferation financing threats. This training enables employees to recognize key red flags, such as unusual financial transactions or suspicious business affiliations, and equips them with the knowledge required to respond appropriately to potential threats. Additionally, the company's training programs are regularly updated to reflect the latest developments in Curaçao's evolving regulatory landscape, ensuring that compliance personnel remain vigilant against emerging risks.

Collaboration with Regulatory Authorities

In its commitment to upholding financial integrity, **Geosix B.V** actively collaborates with regulatory bodies and enforcement agencies, including the Curaçao Gaming Control Board (GCB), the Financial Intelligence Unit (FIU), and other relevant authorities. This collaboration involves sharing intelligence on potential threats, providing timely reports on suspicious activities, and actively participating in industry-wide initiatives aimed at strengthening the iGaming sector's defences against proliferation financing risks. By fostering strong regulatory partnerships, the company plays a vital role in preventing its platform from being misused for unlawful financial activities.

Commitment to Global Security and Compliance

As a responsible iGaming operator, **Geosix B.V** remains unwavering in its dedication to preventing proliferation financing activities within its platform. The company's adherence to Curaçao's latest iGaming regulations and international compliance

frameworks ensures that it upholds the highest standards of financial security, transparency, and legal compliance. These efforts not only safeguard the integrity of the company's financial operations but also contribute to global initiatives aimed at disrupting financial networks linked to WMD development and distribution. By maintaining rigorous compliance controls, the company strengthens its role as a trusted and responsible participant in the international financial system.

III. Risk Assessment of ML & TF

Geosix B.V applies the risk-based approach (RBA) which is a fundamental principle of effective Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies. It ensures that resources are allocated in a manner that mitigates the most significant risks. Under the new Curaçao gaming legislation, implementing a robust RBA is critical for maintaining compliance and enhancing the integrity of the gaming sector. Compliance Officer is responsible for ensuring that RBA is properly implemented and documented. All staff must follow player onboarding procedures that incorporate risk scoring and due diligence requirements.

The new Law on Offshore Games (LOK) framework, replaces the National Ordinance on Offshore Games of Hazard (NOOGH). This legislation mandates stricter AML/CTF measures, requiring the company to maintain a comprehensive RBA to identify, assess, and mitigate money laundering and terrorist financing risks effectively.

Key Components of the Risk-Based Approach

Risk Identification

Geosix B.V recognizes all relevant ML/TF/PF risks based on customer profile, geographical location, game type, payment method, and delivery channel.

Risk Assessment

Geosix B.V conducts a thorough risk assessment that is the cornerstone of the RBA. It conducts regular and comprehensive assessments to identify potential risks associated with their customers, products, services, and geographic locations.

- **Customer Risk:** Evaluate the risk posed by different types of customers. High-risk customers may include politically exposed persons (PEPs), individuals from high-risk jurisdictions, or customers with complex business structures.
- **Product/Service Risk:** Assess the risk associated with different gaming products and services. Higher-risk products may include those with high transaction volumes or anonymous features.
- **Geographic Risk:** Identify risks related to the geographic location of customers and operations. High-risk jurisdictions are those with weak AML/CTF regimes or significant levels of corruption and crime.

Risk Mitigation

Once risks are identified, appropriate mitigation measures are implemented by the company. These measures are proportionate to the level of risk and may include enhanced due diligence, transaction monitoring, and customer verification processes.

- **Enhanced Due Diligence (EDD):** Apply EDD measures for high-risk customers and transactions. This includes obtaining additional information about the customer's source of funds, beneficial ownership, and the purpose of transactions.
- **Transaction Monitoring:** Implement advanced monitoring systems to detect suspicious activities. This involves setting thresholds for alerts and using algorithms to identify patterns indicative of money laundering or terrorist financing.
- **Customer Verification:** Strengthen customer verification processes, especially for high-risk customers. This includes verifying identity through reliable, independent sources and conducting ongoing monitoring of customer activities.

Ongoing Monitoring and Review

Geosix B.V applies continuous monitoring and periodic reviews which are essential to ensure the effectiveness of the RBA. This involves:

- **Transaction Monitoring:** Regularly reviewing transaction data to identify suspicious activities.
- **Customer Profiling:** Updating customer profiles based on new information and transaction history.
- **Policy Review:** Periodically reviewing and updating AML policies and procedures to align with evolving risks and regulatory requirements.

Reporting and Record-Keeping

Effective reporting and record-keeping are critical components of the RBA. The company ensures that all suspicious transactions are reported to the relevant authorities and that records are maintained in accordance with legal requirements.

- **Suspicious Activity Reporting (SAR):** Establish procedures for reporting suspicious activities to the Financial Intelligence Unit (FIU) in a timely manner.
- **Record-Keeping:** Maintain detailed records of customer identification, transaction data, and risk assessments for a minimum period as specified by the legislation. These records must be readily accessible for inspection by regulatory authorities.

Compliance with Curaçao's New Legislation

Under the LOK framework, the company, as a gaming operator in Curaçao demonstrates compliance with the following specific requirements:

- **ML/FT/FP Programs:** Develops and implements ML/FT/FP programs that incorporate the RBA, tailored to the size, nature, and complexity of the business.
- **Training and Awareness:** Provides regular training to employees on ML/FT/FP obligations, focusing on the risk-based approach and how to identify and mitigate risks.
- **Independent Audit:** Conducts independent audits to assess the effectiveness of the ML/FT/FP program and the implementation of the RBA.

Risks Specific to the Gambling Sector

There are certain Risk Areas Specific to the Gambling Sector, the business risk assessment and customer-specific risk assessment are addressed by the company in the following four critical risk areas:

1. Customer Risk

Customer risk involves the potential for money laundering (ML) and terrorist financing (TF) when engaging with certain individuals. This risk is evaluated based on a customer's economic activities and sources of wealth. Specific categories of customers who may pose a higher risk include:

- **Multiple Income Sources:** Customers with various income streams.
- **Irregular Income:** Customers with inconsistent income patterns.
- **Politically Exposed Persons (PEPs):** Individuals holding prominent public roles.
- **High Spenders:** Customers making large expenditures, which may derive from illicit activities.
- **Disproportionate Spenders:** Customers whose spending is inconsistent with their known income or assets.
- **Casual Customers:** Local or tourist patrons whose spending habits fluctuate.
- **Third-Party Involvement:** Use of intermediaries to gamble, purchase chips, or cash out, avoiding customer due diligence (CDD) measures.
- **Multiple Casino Accounts:** Usage of several accounts to mask gambling activities.
- **Anonymous Customers:** Individuals redeeming substantial amounts of chips without proper identification.
- **Junkets:** Operators monitoring player activities and providing credit.

Company's Mitigation Strategies:

- Performs thorough customer due diligence (CDD) for all patrons.
- Implements enhanced due diligence (EDD) for high-risk individuals, including PEPs and significant spenders.
- Continuously monitors and updates customer profiles to reflect their current risk status.
- Enforces stringent verification processes to authenticate the identities of all customers.

- Restricts the use of third-party transactions unless they are validated and justified.

2. Geographical Risk

Location-based risk pertains to the possible dangers a casino faces due to the origin of the player's money and their geographic location. Elements like the player's country of origin, where they live, and where they were born can suggest a higher level of location-based risk. Countries typically considered high-risk include those with inadequate anti-money laundering and counter-terrorism financing systems, widespread corruption, international sanctions for terrorism or the spread of nuclear weapons, and a history of terrorist activities.

Countries at risk can be pinpointed through various channels:

FATF High-Risk Countries: Nations facing a request for action.

FATF Countries Under Enhanced Monitoring: Nations with identified shortcomings.

CFATF Public Statement: Evaluation of risk across regions.

U.S. Department of State's INCSR: Nations marked as Jurisdictions of Concern or Primary Concern. European Commission List: Third-party countries with significant deficiencies in anti-money laundering and counter-terrorism financing.

OFAC Sanctions: Nations subject to specific sanctions.

Credible Sources: Nations that provide financial or support to terrorist groups.

Transparency International's Corruption Perception Index: Nations with high levels of corruption.

Mitigation Strategies applied by the company:

- Keeps a record of countries based on their risk levels.
- Utilizes a variety of trustworthy sources to regularly update and evaluates the risk associated with a player's location.
- Implements stricter due diligence procedures for customers from high-risk areas to reduce the likelihood of potential threats.

Adopting a risk-based approach in ML/FT/FP policies is essential for the company under the new Curacao legislation. By focusing resources on higher-risk areas and continuously monitoring and updating risk assessments, the company can effectively mitigate the risks of money laundering and terrorist financing, ensuring compliance with regulatory requirements and maintaining the integrity of the gaming sector.

3. Product, service & transaction risks

The nature of the gaming industry makes its products and services more vulnerable, hence, easier to exploit by criminals. The issues of customers impacting the outcomes of the games make the industry high-risk due to potential exploitation. Certain

payment methods used by clients and accepted by casinos may pose a very high risk of ML/TF and, consequently, should be treated as high risk factors:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- Anonymous payment methods, such as pre-paid cards and virtual assets;
- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or after minimal play;
- Types of specific games (e.g. roulette, craps → even bets);
- Peer to peer gaming;
- The use by customer of accounts held or cards issued in the name of third parties; The transfer of funds from one gaming account to another;
- Types of financial services (credit/marker, currency exchange, check cashing);
- Multiple casino accounts or wallets (internet operator may own and control multiple web sites); · Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Games involving multiple operators (Poker on platforms shared by multiple operators);
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the casino. This may be useful for dishonest customers who wish to disguise their gambling

In order to mitigate these risks, the company takes the following steps:

- Identity Verification: The usage of modern tools to identify and verify the client.
- Obtains and validates the source of wealth/funds of customers, especially if transactions trigger the set threshold equal to or above 4,000 NAF, cash transactions, large amount transactions (as per the amendment of the NOIS, May 2, 2024).
- Accepts licensed and regulator payment providers.
- Controls and oversees casino accounts to make sure they are used for the purposes of gaming.
- Monitors, controls and regulates peer to peer platforms.
- Ensures the casino account holder details match the details on the card or financial institution account.
- Uses specific fraud detection tools to prevent identity and other types of fraud.
- Monitors transactions, limits cash transactions, verifies users, wallet holders.
- Reports suspicious transactions/activity.
- Educates and trains employees.

4. Distribution channel risks

The risk level may also be determined on the basis of a channel type that is used to establish business relationships:

- Anonymous channels pose higher threats of ML/TF.
- Non face-to-face communication with customers that increases risks of identity theft and impersonation.
- Third-parties serve as intermediaries between customers and casinos, especially if such third-parties are not subject to any AML/CFT requirements.

To tackle the channel risks, the company ensures that:

- Identification and verification of the client's identity.
- Usage of tools that prevent impersonation fraud, validate and verify customers identification documents and the customer.
- Ensures that there are anonymous channels, unregulated third parties involved in the relationship between clients and casino.

5. Technological developments risk assessment

- A Company is maintaining 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 or 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 normally take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. Such risk assessments shall be documented. Where risks are identified, measures must be taken to mitigate these risks.

IV. Clients and players Due Diligence

The company is in line with the requirement that casinos must not have anonymous or fake accounts. They need to identify players and understand the nature of their business relationship. This helps prevent money laundering, terrorism financing, and proliferation. An efficient Customer Due Diligence (CDD) program is crucial for assessing risks and ensuring compliance with expected behaviour. Suspicious activities should be reported to the Financial Intelligence Unit (FIU) and possibly to the Public Prosecutor's Office.

The thresholds that the proprietary anti-fraud system is fed with the view of flagging transactions are based on the following parameters in accordance with the requirements of GCB:

- Transactions are equal to or exceed NAF 4,000.
- Occasional transactions exceed NAF 4,000.
- There is suspicion of money laundering or terrorism financing.
- There are doubts about previously obtained customer identification data.

Transactions can be single or multiple linked transactions surpassing NAF 4,000. Even if individual transactions are below this amount, if linked, they are subject to CDD. Enhanced due diligence is required for high-risk transactions.

Client Due Diligence Measures

Company's CDD measures include:

- Identifying and verifying the player's identity using legit, reliable, independent documents, data, systems.
- Identifying the ultimate beneficial owner and verifying their identity to ensure the casino knows who the owner is. For legal entities, this includes understanding their ownership and control structure.
- Understanding the purpose and nature of the business relationship.
- Conducting ongoing due diligence business relationships and monitoring transactions to ensure they align with the casino's knowledge of the player and their risk profile, including the source of funds if necessary.

Casino staff must not disclose that a report is being made to the FIU, as it could unintentionally tip off players. If there is suspicion of money laundering or terrorism financing, and performing CDD might alert the player, the casino should avoid the process and file a report to the FIU instead.

Geosix B.V. will apply Customer Due Diligence (CDD) measures when a player engages in transactions amounting to or exceeding NAF. 4,000 in a single gaming day. This threshold applies to combined transactions. Full identification and verification procedures must be completed prior to allowing further gaming or financial transactions beyond the threshold.

Company's Identification and Verification of Players

Identification involves collecting personal details to establish a player's identity, while verification confirms these details using reliable documents or data. The extent of information required depends on the risk level.

Player Identification: At a minimum, the following details must be collected:

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

In low-risk scenarios, only the first three details may be needed. For high-risk situations, more information might be required to mitigate money laundering and terrorism financing risks.

Customer Risk Assessment: This assesses potential unusual activity in the business relationship. Initially, a provisional risk rating is assigned based on collected information, which is revised as more data is gathered. This helps determine the appropriate level of CDD as per regulations.

Verification of Identity: Verification ensures a person is who they claim to be by checking reliable documents or data. This typically involves:

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

The aim is to verify the player's identity using clear, legitimate, and good-quality documents, ensuring they are the true owner and the documents are not fraudulent. In cases the casino is still uncomfortable with the quality/quantity of information collected, it takes additional steps requesting additional information such as a player's selfie with their ID or making a first deposit through the account in a regulated financial institution in a reputable jurisdiction.

The company carries out a Customer Risk Assessment

The company carries out this assessment to ensure sufficient information is available to detect unusual activity during the business relationship. At this stage, the company assigns a provisional risk rating based on the initially collected information. This rating is revised once the customer answers questions or provides additional information. Based on the CRA, the company applies the appropriate level of Customer Due Diligence (CDD) as stipulated by the CAP.

The company identifies and verifies the Beneficial Owner

The company ensures that customers register and transact on their own behalf by requiring agreement to terms and conditions and a declaration via tick box. However, it does not rely solely on this and maintains procedures to detect when a player may be acting for others.

Although rare, the company may encounter cases involving beneficial owners—for example, when funds come from a syndicate. In such cases, all contributing individuals are treated as beneficial owners and must be identified and verified.

For corporate accounts or business-related models, the company identifies and verifies the beneficial owners of the registering entities. It distinguishes between standard consumer accounts and business-related accounts.

The company collects verification data for any individual holding 25% or more of shares or voting rights, or anyone with effective control. If none are identified, it verifies the identity of the senior managing official.

Business Relationship Purpose and Nature

The company established the purpose and nature of its relationships with players as a part of its CDD procedure. In the context of the services offered by the company, the purpose of the relationship is obvious, however, in order to determine the risk profile of the client, the company collects sufficient information to ensure it is able to detect any unusual or suspicious activity on players' accounts.

In cases where it is necessary, the company collects source of wealth documentation and expected activity levels. This is required to determine if the activities that generate player's income are legit and whether the income type/level is sufficient to justify the casino account activity. For low and medium risk players, a declaration including some details: employment or business information, salary would be sufficient. In terms of clients of higher risk, independent and reliable sources of wealth are collected by the company.

The described above is collected by the company to determine the model of behaviour of the player used for monitoring purposes and customer's risk profile determination.

Ongoing Identity and Transaction Monitoring

The company's ML/FT/FP policy mandates continuous monitoring of player identities and transactions to detect and prevent money laundering and terrorist financing. This includes regular updates and verification of player identification details, especially for

high-risk individuals, to ensure accuracy and legitimacy. All transactions are scrutinized for unusual patterns or suspicious activities that deviate from established player profiles. Enhanced due diligence is applied to any transactions that meet or exceed the NAF 4,000 threshold, including linked transactions. Additionally, the casino will utilize advanced monitoring systems to flag potential red flags in real-time, ensuring prompt investigation and reporting to the Financial Intelligence Unit (FIU) when necessary. This proactive approach ensures compliance with regulatory requirements and reinforces our commitment to maintaining a secure and transparent gaming environment.

Enhanced Due Diligence

The company's ML/FT/FP policy includes stringent Enhanced Due Diligence (EDD) measures for high-risk scenarios.

When EDD is Required

EDD is mandatory in situations where the risk of ML or TF is higher, including:

- Residents of high-risk jurisdictions – Customers from countries with weak AML/CFT regulations, high corruption levels, or international sanctions require additional scrutiny.
- Politically Exposed Persons (PEPs) – Due to their influence and access to public funds, PEPs pose an increased financial crime risk, necessitating enhanced identity verification and transaction monitoring.
- Use of anonymous financial products – Transactions involving prepaid cards, virtual assets (cryptocurrencies), or other anonymity-enhancing methods require stricter oversight.
- New financial technologies – Any new business practices or financial technologies, such as cryptocurrency transactions or blockchain-based gaming services, must be assessed for potential financial crime risks before implementation.

EDD Measures Implemented by the **Geosix B.V.**

To ensure compliance with ML/FT/FP regulations, EDD measures are proportionate to the risk identified and include:

- Collection of additional customer information, including employment details, previous addresses, and publicly available data.
- Detailed assessment of the business relationship, requiring additional documentation to understand the customer's intent.
- Verification of the source of funds and wealth, ensuring legitimate financial origins (e.g., personal savings, employment income, property sales, inheritances).

- In-depth review of large or unusual transactions, ensuring consistency with expected financial behavior.
- Senior management approval before initiating or continuing a relationship with a high-risk customer.
- Real-time transaction monitoring, with automated alerts on high-risk transactions.
- Ensuring the first deposit originates from a regulated financial institution, registered in the customer's name.
- Ongoing source of funds verification, requiring periodic updates for high-risk customers.

By enforcing these strict measures, **Geosix B.V.** strengthens its financial security framework, ensuring full compliance with international ML/FT/FP standards while mitigating financial crime risks.

Timing of Customer Due Diligence Measures

Geosix B.V. applies Customer Due Diligence (CDD) measures promptly and effectively, ensuring full compliance with ML/FT/FP regulations.

CDD Implementation Based on Transaction Thresholds

At the time of account registration, the company collects and verifies the minimum required personal details of each player, including:

- Full name
- Permanent residential address
- Date of birth
- Politically Exposed Person (PEP) screening
- Sanctions screening

As part of its risk-based approach, the company verifies customer identities before processing financial transactions equal to or exceeding NAF 4,000. This verification process applies to:

- Single transactions that reach or exceed NAF 4,000.
- Multiple linked transactions (deposits, withdrawals, and peer-to-peer transfers) that cumulatively reach NAF 4,000.

To maintain a proactive compliance approach, **Geosix B.V.** continuously monitors all player transactions and calculates the threshold daily, ensuring that all transactions since the business relationship was established are considered.

Upon reaching the NAF 4,000 threshold, the company conducts a comprehensive customer risk assessment, reviewing all relevant data and completing any outstanding CDD obligations.

Proactive Customer Due Diligence Implementation

Geosix B.V. prioritizes early completion of CDD verification, conducting full identity checks at the time of account registration rather than waiting until a financial threshold is met. This reduces the risk of illicit funds entering the gaming system before thorough due diligence has been completed.

Transaction Restrictions While CDD is Pending

If a player reaches the NAF 4,000 threshold before completing full CDD verification, the company applies restrictions to maintain compliance:

- If the threshold is reached due to a deposit, the player cannot deposit or withdraw additional funds but may continue playing with existing account funds.
- If the threshold is reached due to a withdrawal request, the company freezes the account, preventing further gaming activity until verification is complete.

Handling Non-Compliance with CDD Requirements

If a player fails to provide the required CDD documentation within 30 days of reaching the NAF 4,000 threshold **Geosix B.V.** takes the following actions:

- Terminates the business relationship with the player.
- Reports the transaction to the Financial Intelligence Unit (FIU) if there is a presumption of money laundering (ML) or terrorist financing (TF).
- If no suspicion of ML/TF exists, the company returns the funds to the original deposit source (same bank account or digital wallet).
- If ML/TF suspicion is present, the company follows internal procedures to determine whether the funds should be blocked, ensuring full compliance with AML/CTF regulations.

Managing Tipping-Off Risks

Recognizing that blocking an account may raise suspicion, the company carefully evaluates each situation to ensure that necessary compliance actions are taken without violating AML/CTF regulations. Internal procedures guide how cases are handled to prevent inadvertent tipping-off while ensuring regulatory compliance.

By implementing these timely CDD measures, **Geosix B.V.** maintains regulatory compliance, reduces financial crime risks, and ensures the security and transparency of its operations across both online and land-based gaming environments.

Simplified Due Diligence

Our ML/FT/FP policy incorporates Simplified Due Diligence (SDD) measures for low-risk scenarios. SDD is applicable where the risk of money laundering or terrorist financing is minimal. In such cases, the casino may collect a reduced set of customer information, focusing on basic identification details such as full name, date of birth, and residential address. While ongoing monitoring continues, the intensity and frequency of reviews are proportionately lower compared to higher-risk situations. SDD allows for a streamlined verification process, ensuring compliance with regulatory standards while facilitating a smoother and more efficient customer experience for low-risk players. However, should any suspicious activity arise, or if the player's risk profile changes, enhanced due diligence measures will be promptly applied.

Examples of Simplified Due Diligence Measures

- Limited Data Collection – If the risk assessment confirms low ML/TF risk, only basic identity information may be collected, including:
 - Full legal name
 - Date of birth
 - Permanent residential address
- Delayed Verification – In lower-risk cases, verification of identity and beneficial ownership may occur after the business relationship has been established.
- Risk-Based Verification – The level of verification may be adjusted depending on the risk level:
 - In low-risk cases, reliance on alternative reputable data sources may be permitted, even those without photographic identification.
 - Minimal identity verification may be applied if there is sufficient assurance that the customer's identity is legitimate.
- Reduced Frequency of Information Updates – Players categorized as low risk may be subject to less frequent identity verification updates.
- Lower-Intensity Transaction Monitoring – Transactions involving low-risk customers may be monitored less frequently, provided they remain within reasonable monetary thresholds.

Limitations of SDD

SDD cannot be applied in cases where:

- There is a suspicion of ML/TF activity.
- The customer falls into a higher-risk category, in which case Standard Due Diligence (CDD) or Enhanced Due Diligence (EDD) is required.

Politically Exposed Persons

The company's ML/FT/FP policy includes specific measures for dealing with Politically Exposed Persons (PEPs). PEPs, including their family members and close associates, are subject to heightened scrutiny due to the increased risk of involvement in money laundering and corruption. Upon identification of a PEP, Enhanced Due Diligence (EDD) measures are immediately implemented, which include obtaining senior management approval before establishing or continuing the business relationship, comprehensively understanding the source of funds and wealth, and conducting ongoing, rigorous monitoring of all transactions. Detailed risk assessments are performed regularly to detect any suspicious activities, ensuring that our operations remain compliant with regulatory requirements and that the integrity of our gaming environment is upheld.

Reliance on Third Parties and Technological Tools Providers

The company's policy includes specific guidelines for relying on third parties and technological tools providers for the purposes of CDD. When outsourcing elements of the company's due diligence processes or utilizing third-party technological solutions, it is imperative that these entities comply with the same rigorous ML/FT/FP standards mandated by the legislation. Before engaging with any third-party provider, thorough due diligence is conducted to ensure they possess robust ML/FT/FP protocols and a proven track record of compliance. Regular audits and assessments of these third parties are mandatory to verify ongoing adherence to our ML/FT/FP requirements. Contracts with third-party providers must include clauses that obligate them to cooperate with any regulatory inquiries and provide access to relevant data. By implementing these measures, we ensure that our reliance on external partners enhances our ML/FT/FP framework without compromising on security and compliance.

Relationship Termination

If a player is found to be engaged in suspicious activities or fails to provide adequate information during the due diligence process, the casino reserves the right to terminate the business relationship. This decision must be supported by documented evidence and approved by senior management. Upon termination, all account activities must be thoroughly reviewed, and any suspicious transactions reported to the Financial Intelligence Unit (FIU) immediately. The player's access to casino services will be revoked, and their accounts will be closed following regulatory guidelines. Additionally, the casino must ensure that all records related to the terminated relationship are securely stored for at least five years, in compliance with legal retention requirements. This approach ensures that the casino remains vigilant against money laundering and terrorism financing while maintaining compliance with the latest regulatory standards.

Third-Party Reliance for Customer Due Diligence

Geosix B.V. may engage third parties to perform specific aspects of Customer Due Diligence (CDD); however, this reliance is subject to strict regulatory oversight to ensure full compliance with ML/FT/FP requirements. Despite delegating certain CDD functions, the company retains ultimate responsibility for ensuring that all CDD measures are properly implemented and adhered to. To maintain compliance, the company ensures immediate access to all customer identification details provided by the third party upon request. Additionally, formal agreements with these third-party providers are established, outlining clear obligations for data provision, adherence to AML regulations, and periodic compliance testing.

Even when CDD procedures are outsourced, **Geosix B.V.** remains directly responsible for conducting independent risk assessments, determining Politically Exposed Person (PEP) status, and maintaining ongoing transaction monitoring to detect any suspicious activities. Third-party providers engaged in CDD processes must be regulated entities subject to AML/CFT laws and regulatory supervision. Furthermore, the third party must maintain an independent business relationship with the customer, separate from its relationship with GAMEPLAY INTERNATIONAL B.V. To mitigate jurisdictional risks, the company conducts a comprehensive risk assessment of the third party's country of operation, ensuring compliance with international risk intelligence reports.

There is a distinction between third-party reliance and outsourcing. In third-party reliance, the external provider conducts specific CDD elements independently, but **Geosix B.V.** remains fully accountable for compliance. In outsourcing scenarios, the third party applies CDD procedures strictly under the company's internal policies and regulatory framework, with full oversight remaining with **Geosix B.V.** Regular quantitative and qualitative assessments are conducted to evaluate the effectiveness of the service provider, ensuring that customer risk assessments and business relationship decisions remain solely within the company's control.

By enforcing strict oversight and regulatory compliance in third-party CDD processes, **Geosix B.V.** effectively mitigates risks while ensuring a secure, transparent, and legally compliant gaming operation.

On-Going Monitoring

The Company is conducting ongoing due diligence on business relationships and scrutinizing transactions throughout the course of those relationships. This ensures consistency with the Company's knowledge of the customer, the customer's business, and their risk profile.

Ongoing Monitoring of Identity

The Company is maintaining accurate and up-to-date identification data for its customers. Since a customer's identity may change over time, the Company is ensuring that any such changes are detected and re-verified. This includes obtaining updated evidence of identity periodically, refreshing data after key events (such as a change in payment instrument), or tracking the expiry dates of identification documents and updating them as necessary. The Company is assessing, on a risk-sensitive basis, whether changes are substantial enough to require a reassessment of the customer's risk profile.

Ongoing Monitoring of Transactions

The Company is monitoring transactions to prevent involvement in money laundering (ML) or terrorist financing (TF), and to safeguard its reputation. When reviewing transactions, if the Company notices any activity that does not align with what it knows or expects from the customer, it is required to question that activity. In such cases, the Company is identifying the source of the funds used in the transaction. The source of funds refers to how the customer obtains the money for that specific transaction.

Application of CDD measures to existing customers

The company applies Customer Due Diligence (CDD) measures to existing customers based on risk and materiality. It reviews whether current procedures meet CDD obligations and, if so, continues using them while ensuring effective ongoing monitoring.

If no CDD procedures were previously in place, the company implements them on a risk-sensitive basis and conducts due diligence on existing relationships at appropriate times.

Review of Existing Customer CDD Compliance

- Ongoing Due Diligence – The company continuously applies CDD measures to existing customers, with a particular focus on transaction monitoring and risk reassessment.
- Risk-Sensitive Approach – For existing customers where prior CDD procedures were inadequate or incomplete, the company:
 - Conducts retrospective CDD, prioritizing higher-risk customers.
 - Performs periodic CDD updates to align with ML/FT/FP regulations.

When CDD is Reapplied to Existing Customers

Geosix B.V. reassesses existing customers when:

- A customer's risk profile changes significantly (e.g., sudden large transactions, change in jurisdiction, PEP status).

- Regulatory updates or legal requirements mandate a reassessment of customer data.
- An existing customer engages in transactions equal to or exceeding the NAF 4,000 threshold, triggering full CDD verification.

Compliance for Previously Unverified Customers

If a customer was previously onboarded without formal CDD procedures, the company:

- Implements full CDD measures, prioritizing high-risk customers.
- Conducts customer verification at appropriate intervals, using a risk-sensitive approach.

By ensuring that existing customer relationships comply with ML/FT/FP regulations, **Geosix B.V.** reinforces its commitment to financial security and prevents money laundering and terrorist financing risks.

V. Sanctions

The ML/FT/FP policy mandates strict adherence to international sanctions and regulatory measures. We are committed to implementing comprehensive procedures to ensure compliance with all applicable sanctions imposed by national and international authorities. This includes conducting rigorous due diligence on all clients and transactions to prevent dealings with sanctioned individuals, entities, or jurisdictions, screen all players against UN, EU, and Curaçao sanctions lists before onboarding and periodically thereafter. If a match is found, the player's funds shall be frozen immediately and reported to the Financial Intelligence Unit (FIU) Curaçao without alerting the customer. Our policy requires ongoing monitoring and immediate reporting of any suspicious activities that may violate these sanctions. Additionally, our ML/FT/FP framework encompasses regular training for all relevant personnel to ensure a thorough understanding of and compliance with the latest sanctions regulations, thereby safeguarding the integrity of our operations and mitigating any associated risks.

The company is committed to ensuring that all transactions and client engagements are meticulously screened against updated Sanctions Lists to prevent involvement with individuals or entities subject to sanctions. This involves implementing automated systems for real-time checks and maintaining an updated database to reflect the latest sanctions information. Any matches or suspicious activities identified must be reported immediately to the relevant authorities, and appropriate measures, including account freezes or transaction blockages, will be enforced to mitigate any compliance risks. Regular reviews and updates of our sanctions compliance procedures will be conducted to align with evolving legislation and ensure robust ML/FT/FP practices.

Such lists include but are not limited to:

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

The company's due diligence processes are designed to uncover any indirect or covert attempts to engage with sanctioned parties or jurisdictions. Any identified evasion tactics will be promptly reported to the relevant authorities, and immediate corrective actions will be taken, including the suspension of transactions and the review of affected accounts. Regular audits and staff training will ensure ongoing vigilance and adherence to the latest legislative requirements and best practices in combating sanctions evasion.

VI. Suspicious Activity Reporting

Recognition and Reporting of Unusual Activity

The company makes sure it diligently recognizes and reports unusual activity that may indicate potential money laundering or terrorist financing. Unusual activity includes, but is not limited to, deviations from a client's known behavior or transactional patterns, frequent high-value transactions, or transactions involving high-risk jurisdictions. Employees are required to be vigilant and report any such activities immediately to the designated Officer. The Compliance Officer will then conduct a thorough investigation to determine whether the activity warrants further action or reporting to relevant authorities.

Recognition and Reporting of Unusual Transactions

The following transactions or intended transactions are deemed unusual:

- a Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.
- b Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c Transactions in the amount of NAF. 5,000 or more, regardless of whether the transaction is made by check or other form of payment, or through electronic or other non- physical means.
- d Frequent high-value deposits followed by minimal play.
- e Structuring deposits to avoid reporting thresholds.
- f Use of third parties to obscure true ownership of funds.

This includes but is not limited to:

Accepting or releasing a deposit in the amount of NAF. 5,000 or more at the request of the client.

Sale to a customer of chips in the amount of NAF. 5,000 or more. "Chips" include but is not limited to tokens and credits.

A pay out in the amount of NAF. 5,000 or more

Prohibition of Disclosure

To maintain the integrity of the reporting process and comply with legal obligations, our policy strictly prohibits the disclosure of any information related to suspicious activity reports (SARs) to the subjects of such reports or unauthorized parties. This prohibition is crucial to prevent potential interference with ongoing investigations or legal proceedings. Employees are required to handle all related communications discreetly and are only permitted to discuss SARs with the Compliance Officer or other authorized personnel. Any breach of this confidentiality requirement will be treated as a serious violation of our ML/FT/FP policy and may result in disciplinary action. This ensures that the reporting process remains confidential and effective in addressing potential threats.

VII. Compliance Officer

There is a designated and qualified individual who serves as the Compliance Officer within the company. The appointment of the Compliance Officer is a critical element of our Anti-Money Laundering (AML) framework and is made by the senior management to ensure both the independence and authority of the role. The selected Compliance possesses relevant experience and expertise in AML compliance and be sufficiently senior to oversee the implementation of AML policies and procedures. This appointment is formalized through a documented appointment letter outlining the scope of their duties and the reporting structure within the organization.

Functions

The Compliance Officer is tasked with several key functions to ensure the effective operation of our AML program. Their primary responsibilities include overseeing the implementation of AML policies and procedures, ensuring compliance with all relevant regulations, and acting as the central point of contact for all AML-related matters. The Compliance Officer is responsible for reviewing and approving the organization's AML policies to ensure they meet current regulatory standards and effectively address emerging risks. Additionally, they oversee the AML training program for employees, ensuring that all staff are adequately educated on AML requirements and their roles in maintaining compliance.

Responsibilities

The Compliance Officer holds significant responsibilities within our AML framework, including:

1. **Monitoring and Reporting:** The Compliance Officer is responsible for the continuous monitoring of transactions and client activities to identify and investigate suspicious activities. They are required to file Suspicious Activity Reports (SARs) to the Financial Intelligence Unit (FIU) as needed and maintain accurate records of these reports.
2. **Policy Development:** Developing and updating the organization's ML/FT/FP policies and procedures in line with the latest Curaçao gaming legislation and international best practices. This includes adapting the ML/FT/FP framework to address new risks and regulatory changes.
3. **Training and Awareness:** Ensuring that all employees receive appropriate ML/FT/FP training and are aware of their responsibilities in detecting and reporting suspicious activities. The Compliance Officer regularly reviews and updates the training materials to reflect any changes in legislation or internal policies.
4. **Liaison with Authorities:** Acting as the primary liaison with regulatory bodies, law enforcement, and other relevant authorities concerning ML/FT/FP issues. This includes responding to requests for information and participating in regulatory inspections or audits.
5. **Compliance Oversight:** Conducting periodic reviews and audits of the ML/FT/FP program to ensure its effectiveness and compliance with legal requirements. The Compliance Officer must also address any deficiencies identified during these reviews and implement corrective actions as necessary.
6. **Documentation and Record-Keeping:** Maintaining comprehensive records of all ML/FT/FP activities, including SARs, internal reports, training sessions, and policy updates. These records must be kept in accordance with legal requirements and be readily accessible for review by regulatory authorities.

By fulfilling these functions and responsibilities, the Compliance Officer plays a crucial role in safeguarding the organization against money laundering and terrorist financing risks, ensuring robust compliance with Curaçao's ML/FT/FP legislation.

VIII. ML/FT/FP Audit

In adherence to the new Curacao gaming legislation, the company is required to undergo an independent Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF) and Counter-Proliferation Financing (CPF) audit. This chapter outlines the framework for conducting such audits, the roles of independent audit functions, and the examination process by the Gaming Control Board.

Independent Audit Function

The primary purpose of an independent annual ML/FT/FP audit is to assess the effectiveness and compliance of the entity's ML/FT/FP policies and procedures. The annual audit is critical for ensuring that the organization adheres to the latest legal standards and best practices in mitigating risks related to money laundering and terrorism financing. The scope of the audit includes a comprehensive review of the ML/FT/FP program, risk assessments, transaction monitoring systems, staff training programs, and reporting mechanisms.

The company engages with an adequately resourced internal audit or an independent auditor who is not only certified but also possesses expertise in ML/FT/FP compliance on an annual basis. The auditor must be independent of the organization's AML Compliance staff to avoid any conflicts of interest. The selection process should be transparent and include consideration of the auditor's experience, qualifications, and reputation in the industry. The chosen auditor should be approved by the Gaming Control Board to ensure they meet the regulatory requirements set forth in the Curacao gaming legislation.

Audit Procedures

The independent audit is conducted in accordance with international auditing standards and the specific requirements outlined by the Curacao Gaming Control Board. The audit procedures should include, but are not limited to:

- Review of ML/FT/FP Policies and Procedures: Ensure they are current and aligned with legal requirements.
- Assessment of Risk Management Framework: Evaluate the adequacy of risk assessments and mitigation strategies.
- Examination of Transaction Monitoring Systems: Verify the effectiveness of systems designed to detect and report suspicious activities.
- Evaluation of Staff Training Programs: Assess the comprehensiveness and effectiveness of training provided to employees.
- Audit of Reporting Mechanisms: Review the processes for reporting suspicious transactions and compliance issues.
- Review of the Customers' Files: Ensure company's compliance with KYC/KYB/CDD procedures.

Auditor Reporting

Upon completion of the audit, the independent auditor must prepare a detailed report outlining findings, recommendations, and any identified deficiencies. This report

should be submitted to the organization's senior management and the Gaming Control Board. The organization is required to respond to the auditor's recommendations and implement corrective actions within a specified timeframe. Follow-up audits may be conducted to ensure that corrective measures have been effectively implemented.

Examination by the Gaming Control Board

Geosix B.V. is aware that the Gaming Control Board is responsible for overseeing the ML/FT/FP compliance of all licensed entities. This includes reviewing the results of independent audits and conducting its own examinations to ensure adherence to regulatory requirements. The Board has the authority to request additional documentation, conduct onsite inspections, and review the implementation of audit recommendations.

The examination process by the Gaming Control Board involves several key steps:

- **Review of Audit Reports:** The Board will analyze the independent auditor's report to assess the entity's compliance and identify any areas of concern.
- **Onsite Inspections:** The Board may perform onsite inspections to verify the accuracy of the audit findings and the effectiveness of implemented measures.
- **Interviews and Documentation Review:** The Board will conduct interviews with key personnel and review relevant documentation to gain a thorough understanding of the entity's ML/FT/FP practices.

Entities found to be non-compliant with ML/FT/FP regulations, based on audit findings or the Board's examination, may face regulatory sanctions. These sanctions can range from fines and operational restrictions to suspension or revocation of the gaming license. The company works closely with the Gaming Control Board to ensure, if required, that corrective actions are taken and will monitor compliance to prevent future violations.

IX. Employee screening program and training

ML/FT/FP training is tailored to employees' specific function and provided to all employees, including but not limited to:

- Senior management
- Compliance officers
- Customer-facing staff, VIP managers
- Operational staff
- Any other employees involved in financial transactions or customer interactions

Initial training is provided to all new employees upon hire. Additionally, all employees receive regular refresher training at least annually. More frequent training sessions

may be required for roles with higher exposure to money laundering and terrorism financing risks.

The training program covers the following topics:

- Overview of ML/FT/FPF laws and regulations in Curacao
- Internal ML/FT/FP policies and procedures
- Employee roles and responsibilities in ML/FT/FP compliance
- Identification and verification of customers (KYC/CDD procedures)
- Recognizing and reporting suspicious activities and transactions
- Record-keeping and documentation requirements
- Consequences of non-compliance for both the individual and the organization
- Recent trends and typologies in money laundering and terrorism financing

Training can be delivered through various methods to ensure effectiveness and accessibility, including:

- In-person workshops and seminars
- Online courses and webinars
- Interactive e-learning modules
- Case studies and practical exercises
- Role-playing scenarios

A combination of these methods is used to address different learning styles and to reinforce the training material.

The primary objective of ML/FT/FP training is to equip employees with the knowledge and skills necessary to detect and prevent money laundering and terrorism financing activities. Training ensures that employees understand their legal obligations, recognize suspicious activities, and are aware of the internal procedures for reporting such activities. A well-informed workforce is crucial for the effective implementation of ML/FT/FP policies and contributes to the integrity and reputation of the gaming industry.

X. Record Keeping Procedure

The company maintains all necessary records of both domestic and international transactions for a minimum period of five years, ensuring its ability to comply with information requests from the appropriate authorities. These records are detailed enough to enable the reconstruction of individual transactions—including the amounts and types of currency involved—so they may serve as evidence in criminal investigations or prosecutions if required.

Additionally, the company retains all documentation obtained through Customer Due Diligence (CDD) measures—such as copies of official identification documents (e.g.,

passports, identity cards, driver's licenses), account files, and business correspondence—for at least five years following the end of the business relationship or the completion of an occasional transaction.

All CDD information and transaction records are made available to domestic competent authorities when requested, in accordance with applicable legal requirements.

XI. Senior Management Obligations & Responsibilities

The Company's senior management holds a central role in identifying, assessing, and managing the inherent risks associated with money laundering, terrorist financing, and proliferation financing (ML/FT/FP). The Board of Directors requires that a designated AML/CFT Officer provide regular updates on any material deviations within the control environment. This officer is also responsible for submitting an annual report evaluating the effectiveness of the Company's systems and controls in mitigating ML/FT/FP risks.

To maintain a strong compliance posture, senior management ensures that all relevant policies and procedures undergo comprehensive review at least once per year. These reviews are informed by monthly risk assessments, enabling the timely detection of potential control gaps or weaknesses in risk mitigation strategies. Where deficiencies are identified, the AML/CFT Officer is authorized to recommend corrective measures for Board approval, reinforcing the Company's commitment to a dynamic and responsive risk management framework.

In alignment with international best practices, senior management also oversees the implementation of comprehensive training programs for employees. These programs are tailored to promote a deep understanding of ML/FT/FP threats, ensuring that all staff—particularly those in sensitive or high-risk roles—are equipped to recognize and respond to suspicious activities appropriately.

Moreover, senior management is responsible for ensuring the Company's internal control structure is both effective and resilient. This includes enforcing clear segregation of duties, well-defined authorization protocols, ongoing monitoring mechanisms, and thorough documentation standards. To support continuous improvement, the Company conducts regular independent audits and evaluations of its ML/FT/FP program to objectively assess performance, identify enhancement opportunities, and uphold full compliance with applicable regulatory obligations.

Annex 1 – Definitions

AML (Anti-Money Laundering) – A set of laws, regulations, and procedures designed to prevent money laundering and other financial crimes.

CTF (Counter-Terrorism Financing) – The process of identifying and preventing financial transactions that support terrorist activities.

CPF (Counter-Proliferation Financing) – Measures aimed at stopping financial support for the spread of weapons of mass destruction.

KYC (Know Your Customer) – Procedures used to verify the identity of customers and monitor their financial activities.

CDD (Customer Due Diligence) – A process of verifying customer identity, assessing risk, and monitoring transactions to detect potential illicit activity.

EDD (Enhanced Due Diligence) – Additional verification and risk assessment measures applied to high-risk individuals, businesses, or transactions.

UBO (Ultimate Beneficial Owner) – The individual who ultimately owns or controls an account or financial transaction.

SOF/SOW (Source of Funds/Source of Wealth) – Verification of the origin of financial assets to ensure they are not derived from criminal activities.

PEP (Politically Exposed Person) – An individual holding a high-profile political or public function who requires additional scrutiny due to increased financial crime risks.

SAR/STR (Suspicious Activity Report/Suspicious Transaction Report) – A report submitted to regulatory authorities when a transaction or financial activity appears suspicious or unusual.

FIU (Financial Intelligence Unit of Curaçao) – The national agency responsible for analyzing and processing reports on suspicious financial transactions.

BoD (Board of Directors) – The company's governing body responsible for compliance oversight, corporate governance, and regulatory adherence.

Compliance Officer – A senior official responsible for managing ML/FT/FP risks, ensuring compliance with financial crime regulations, and operating independently from gaming operations.

NOOGH (National Ordinance on Offshore Games of Hazard) – Curaçao's legislative framework governing offshore gaming activities.

OFAC (Office of Foreign Assets Control) – A U.S. Treasury Department agency that enforces economic sanctions against targeted individuals, entities, and countries.

FATF (Financial Action Task Force) – An international organization that develops and promotes global AML and CTF standards and monitors high-risk jurisdictions.

CFATF (Caribbean Financial Action Task Force) – A regional group of Caribbean, Central, and South American countries dedicated to combating money laundering and terrorist financing.

EU (European Union) – A political and economic union that enforces AML/CTF directives among its member states.

UK (United Kingdom) – A jurisdiction with AML/CTF regulations overseen by its financial and regulatory authorities.

US (United States) – A country with financial crime oversight conducted by agencies such as OFAC and FinCEN.

Risk-Based Approach (RBA) – A methodology for assessing and managing AML/CTF risks based on transaction types, customer profiles, and jurisdictions.

Blacklist – A list of individuals, businesses, or jurisdictions subject to financial restrictions due to regulatory concerns.

Sanctions – Legal restrictions imposed on specific countries, individuals, or entities due to financial crime, national security risks, or geopolitical concerns.

Automated Screening Tools (AST) – Software that screens customers against sanctions lists and flags high-risk individuals or transactions.

Economic Sanctions – Financial and trade restrictions imposed by governments or regulatory bodies to restrict illicit financial activity.

Curaçao Gaming Control Board (GCB) – The primary supervisory authority responsible for overseeing AML/CTF compliance in the gaming sector.

Know Your Business (KYB) – The process of verifying business entities, their ownership structures, and financial activities for compliance purposes.

Structuring – A money laundering technique that involves breaking large transactions into smaller amounts to evade reporting thresholds.

Layering – A method used to disguise the source of illicit funds by conducting multiple, complex transactions.

Integration – The final stage of money laundering, in which illicit funds are reintroduced into the legitimate economy.

Sanctions Evasion – Attempts to circumvent restrictions by disguising transactions involving sanctioned individuals, entities, or countries.

Financial Action Task Force (FATF) – A global authority that sets AML/CTF compliance standards and issues blacklists and greylists for high-risk countries.

First Line of Defense – Employees responsible for collecting customer information and identifying suspicious activity during onboarding and transaction processing.

Suspicious Transaction Report (STR) – A report submitted to regulatory authorities when a transaction raises AML/CTF concerns.

Egmont Group of FIUs – An international network of Financial Intelligence Units that facilitates cooperation and intelligence-sharing in financial crime investigations.

The Wolfsberg Group – An association of major global banks that develops best practices for private banking AML compliance.

Money Laundering Reporting Officer (MLRO) – The designated officer responsible for overseeing AML policies, conducting transaction monitoring, and submitting SARs/STRs.

Audit Logs – Records maintained for compliance and regulatory review, documenting AML/CTF efforts and stored for a minimum of five years.

Reporting Mechanism Audit – A process that ensures SARs and other compliance reports meet legal standards and are properly documented.

Unusual Transaction – A financial activity that deviates from normal transaction patterns and may indicate illicit activity.

Transaction Monitoring – The real-time analysis of financial transactions to identify suspicious behavior and detect money laundering risks.

High-Risk Third Country – A jurisdiction identified by FATF or the European Commission as having insufficient AML/CTF controls.

Comprehensive Sanctions – The strictest level of sanctions, prohibiting all financial dealings with a sanctioned country, individual, or entity.

Sanctions Compliance and Screening – The process of verifying customers and transactions against international sanctions lists to prevent illicit financial activity.

Operational Restrictions – Limitations imposed on businesses that fail to comply with AML/CTF regulations, including license suspensions and financial penalties.

Risk Appetite – The level of risk an organization is willing to accept within its AML/CTF compliance framework.

Beneficial Owner – The individual who ultimately controls or benefits from a financial transaction or legal entity.

Financial Crime Prevention Framework – A structured program designed to mitigate money laundering, terrorist financing, and other financial crimes.

Customer File Review – A compliance practice where customer records are periodically examined to ensure adherence to KYC, CDD, and regulatory requirements.

Senior Management Oversight – The responsibility of executive leadership to ensure that ML/FT/FP programs are effectively implemented and continuously improved.

Training and Awareness Programs – Educational initiatives designed to ensure employees understand AML/CTF risks, compliance obligations, and reporting procedures.

Ongoing Monitoring – A continuous review of customer transactions and risk profiles to identify potential financial crime risks.

Regulatory Reviews – Assessments conducted by supervisory authorities to verify that a company's AML/CTF policies and practices meet legal requirements.

Corrective Action Plans – Compliance strategies implemented in response to audit findings or regulatory enforcement actions.

Periodic Independent Audits – External reviews of a company's ML/FT/FP compliance framework to identify gaps and improve regulatory adherence.

Internal Control Mechanisms – Policies and procedures designed to safeguard against financial crime risks and ensure compliance with AML regulations.

Real-Time Risk Assessment – The use of technology and compliance teams to assess and respond to potential money laundering threats as transactions occur.

Confidentiality in Reporting – The requirement to protect information related to SARs/STRs, preventing unauthorized disclosure or tipping off of customers.