

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)**

Version 2

Approved by:
Geosix N.V Executive Board
9th of December 2025



Responsible Compliance Officer:
Semen Klyuchyk
compliance@geosix.net

Contents

1. Introduction and Policy Statement	4
2. iGaming Landscape	4
3. Abbreviations	5
4. Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction	6
5. Integration of National Risk Assessment	9
5.1 Risk Score Calculation	10
5.2 Ongoing Monitoring and Review	11
6. Risk- Based Approach	13
6.1 Product, Service, and Transaction Risks	14
6.2 Geographical Risk	15
6.3 Distribution Channel Risks and Mitigation Measures	15
6.4 Technological Developments Risk Assessment	16
6.5 Implementation of Risk Mitigation Strategies	17
6.6 Sector-Specific Risks in iGaming	18
7. Client Due Diligence Guidelines and Acceptance Policy	21
7.1 The company applies CDD measures	22
7.2 To establish a player's identity, the following information will be collected:	22
7.3 Timing of Client Due Diligence Measures	23
7.4 Ongoing Review and Risk-Based Monitoring	25
7.5 Termination of Business Relationships	26
7.6 Third-Party Reliance for Client Due Diligence	26
7.7 The company identifies and verifies the Beneficial Owner	27
8. Transaction On-Going Monitoring	28
8.1 Transaction monitoring system	29
9. Politically- Exposed Persons (PEPs)	30
10. Sanctions Management, FATF High-Risk List, License Restrictions	31
11. Suspicious Activity Reporting	32
11.1 Objective and Subjective Indicators (NORUT Compliance)	33
11.2 Integration of FIU Ministerial Indicator Decree	33
11.3 Reporting Unusual Transactions "Without Delay"	34
11.4 Identifying Unusual Transactions	34
12. Compliance Officer	36

13. Senior Management Obligations & Responsibilities	37
14. Employee Training and Screening Program	38
15. Record- Keeping Procedure	40
16. AML/CFT/CPF Audit	41
17. Regulatory Access and Legal Force	43
18. Appendixes	45
Appendix I Player Risk Scoring Assessment	45
Appendix II Employee Screening Programme	46
Appendix III Sanctions Policy	50
Appendix IV Client Acceptance Policy	58

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

1. Introduction and Policy Statement

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 licenses 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.

The Company hereby acknowledges and affirms that it is fully bound by the Regulations for the Combatting of Money Laundering, Terrorist Financing, and Proliferation Financing for the Purpose of the National Ordinance on the Supervision and Regulation of the Gaming Sector, which became legally effective on 1 January 2025. These Regulations apply directly and in full to all Curaçao-licensed gaming operators and impose mandatory obligations regarding governance, customer due diligence, monitoring, reporting, recordkeeping, independent audit, compliance staffing, and risk-based operational conduct.

The Company explicitly recognizes that compliance with these Regulations is not discretionary, is a condition of its OGL license, and forms part of the regulatory obligations enforced by the Curaçao Gaming Control Board (GCB). All internal AML/CFT/CPF policies, systems, and controls are therefore updated, implemented, and maintained to ensure continued alignment with the January 2025 regulatory framework.

2. 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) (LOK), 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.

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 clients or the external payment providers to help them bypass internal safeguards.

3. Abbreviations

AML – Anti-Money Laundering

Compliance Officer – Anti-Money Laundering Compliance Officer

BoD – Board of Directors of the Company

CDD - Client Due Diligence

EDD - Enhanced Due Diligence

CFT- Combating the Financing of Terrorism

EU – European Union

FATF – Financial Action Task Force

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

PEP- Politically Exposed Person

UN- United Nations

CPF Counter-Proliferation Financing

LOK – National Ordinance on the Supervision and Regulation of the Gaming Sector

NOPML – National Ordinance Penalization of Money Laundering

NORUT – National Ordinance on Reporting of Unusual Transactions

2025 AML/CFT/CPF Regulations – Regulations for the Combatting of ML/TF/PF (effective 1 Jan 2025)

4. 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 withdrawals.

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.

Terrorist- 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 deposits, transactions involving high-risk industries, or activities designed to evade detection by financial institutions.

Proliferation Financing

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.

5. Integration of National Risk Assessment

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.

5.1 Risk Score Calculation

Money laundering and terrorist financing risks are measured by using a number of factors listed above. **Geosix B.V** uses the application of risk categories to clients/situations to provide a strategy for managing potential risks and it enables the Company to subject clients to proportionate due diligence and ongoing monitoring. The weight given to these criteria in assessing the overall risk of the client and risk score assigned is as follows:

Category	Score	Level of Due Diligence	Approval Process
Low Risk	0-1.5	Standard Due Diligence	Client Service/Compliance Officer
Medium Risk	1.5.-2.4	Standard Due Diligence	Client Service/Compliance Officer
High Risk	2.4 or more	Enhanced Due Diligence	Annual and approval from Compliance Officer
Unacceptable	Any of the factors that are not accepted by the company	Automatically Reject	Automatically Reject

The Risk Score correlates with the level of due diligence imposed on the client and who is responsible for conducting due diligence. Regardless of the risk rating, **Geosix B.V** performs automatic PEP, sanctions and, adverse media screening on all clients as part of the client due diligence process and ongoing risk assessment, ensuring the Firm meets its regulatory requirements and obligations. Further, **Geosix B.V** uses risk score in order to determine the different treatments of identification, verification, additional client information, and monitoring for each client as follows:

Low – Standard Due Diligence applies. Clients in this category present an overall low risk to the Company, however, because of the high-risk nature of online gambling Company will not apply Simplified Due Diligence.

Medium – Standard Due Diligence applies. Clients in this category present an overall medium risk to the Company.

High – Enhanced Due Diligence applies. Clients in this category present an overall high risk to the Company. These clients will be reviewed by the Compliance Officer and

approval or rejection. and final sign-off. Some of the high-risk clients include, but are not limited to:

- the business relationship is conducted in unusual circumstances
- the transaction is complex or unusually large compared to the profile of the client or to other clients of similar type/category
- clients that are resident in geographical areas of higher risk or sanctioned countries
- a client has been identified to be a Politically Exposed Person (“PEP”) or family member or close associate of a PEP. See section on PEPs below.
- clients receive a high-risk score at the onboarding stage. See Player Risk Scoring Assessment. **Appendix I.**
- clients that receive high-risk scores based on multiple factors described in this procedure (adverse media, a large deposit, and so forth)
- the client has provided false or stolen identification documents or other information on establishing the relationship
- transaction(s) have no apparent economic or legal purpose
- companies that offer financial services or offer services to underlying clients or have underlying clients in any capacity, excluding liquidity providers.
- in combination with other factors, clients with deposit amount over lifetime throughout the entire relationship with the client

Unacceptable Clients

- Person or entities subject to financial sanctions or have been engaged in money laundering activities
- **Geosix B.V** is required to adhere to the sanction’s regime, which is designed to deny services and gambling products to individuals who are deemed to be a high Money Laundering or Terrorist Financing risk. As a result, **Geosix B.V** is prohibited to enter in any business relationship with individuals or entities listed as targets for financial sanction.
- Individuals under the age of 18 years old. **Geosix B.V** requires an individual to be at least 18 years old to open an account with the Firm. All individuals under 18 years of age will be automatically rejected.
- Individuals with unknown or unverified wealth sources
- Gameplay matching knows fraudulent patterns

5.2 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.

Screening of clients against PEP, Sanctions, and Adverse Media on a regular basis. Any alerts considered to be true matches may trigger a Reviews Triggered by Specific Events

Reviews Triggered by Specific Events

Certain events will trigger an Event-Driven Review which may, depending on the type of changes flagged, require a full customer due diligence refresh.

Geosix B.V. through the course of its daily activities, obtains the information that brings a question to the accuracy of the customer due diligence information collected, or if suspicion arises, then the customer will undergo an immediate review, irrespective of their risk status.

Regularly Conducted Reviews

Geosix B.V. has an obligation to ensure that customer due diligence information is relevant and kept up to date via regular client reviews. The extent to which clients' reviews are undertaken will be determined by using a risk-based approach and applied in accordance with the risk rating applied to the customer during the customer risk assessment. The Company has a customer review process based on the High, Medium, and Low risk factors assigned to its customers

Regularly Conducted Reviews are conducted in line with the client's risk score and profiles as follows.

High Risk – Every year. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse news
- Complete review of transaction profile, including new products requested

Medium Risk – Every two years. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse media
- Complete review of transaction profile, including new products requested

The information obtained during the review will be assessed to determine if the medium risk rating still applies.

Low Risk – Every three years. However, reviews will be undertaken when trigger events occur such as:

- where the firm had come into possession of news or information that brings doubt to the accuracy of the current CDD information held
- when the Firm has identified activity deemed to be suspicious
- This review will entail establishing the following:
 - Re-confirmation of Address
 - Screening for adverse media
- The information obtained during the renewal will be assessed to determine if the low-risk rating still applies.

The company's procedures are reassessed whenever the National Risk Assessment (NRA) is updated, ensuring that internal controls, risk ratings, and related measures remain aligned with current national risk priorities and regulatory expectations. Confirm procedures are reassessed whenever the NRA is updated.

6. Risk- Based Approach

Company applies a risk-based approach in combating exploitation of its online platform for the purposes of ML and TF. The methodology the Company adopts is based on the Guidance of the Financial Action Task Force (FATF) as regards ML/ TF Risk Assessments and determines a risk level by evaluating types of risk, threats, vulnerabilities, controls, consequences, the likelihood of it happening, and the impact it may have on the business model in a particular geographical location.

Geosix B.V. conducts a formal Business Risk Assessment (BRA) annually and upon any significant operational change. This BRA evaluates money laundering and terrorism financing risks associated with clients, products, delivery channels, geographical exposure, and technological developments. The assessment is documented, approved by the Board of Directors, and revised in accordance with the latest regulatory updates or business model changes

Specifically, AML/CFT risk assessment categories center around the risks associated with:

Risk Factors

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

Certain client types are considered to carry a higher risk of financial crime involvement. This includes individuals with multiple income streams, which can complicate the verification process of fund legitimacy. Clients with fluctuating or unpredictable financial behavior may also increase the risk due to the challenge in assessing their financial patterns. Politically

Exposed Persons (PEPs) are subject to intensified scrutiny owing to their potential influence over public funds and associated corruption risks.

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

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

6.1 Product, Service, and Transaction Risks

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

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

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

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

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

Factors considered to evaluate Transaction Risk:

- Account monitoring (deposit, withdrawals and account activity)
- Transaction monitoring (activity and analysis screening results for deposits and withdrawals)
- Transaction monitoring to track specific patterns in client' activities and detect fraud

Factors considered to evaluate Product or Services Risk:

- Risk typologies associated with each product or service
- The level of transparency, or opaqueness, the product, service, or transaction affords
- The complexity of the product, service, or transaction
- The value or size of the product, service, or transaction

6.2 Geographical Risk

Geographical risk is determined by the location of a client and the origin of their financial resources, which may indicate elevated exposure to ML, TF, or Counter-Proliferation Financing (CPF) threats. Jurisdictions associated with weak AML/CFT controls, high corruption levels, or international sanctions pose heightened risk. Countries identified in relation to terrorism or weapons proliferation are subject to strict oversight.

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

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

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

6.3 Distribution Channel Risks and Mitigation Measures

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

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

By applying rigorous monitoring procedures and ensuring secure authentication across all distribution points, Geosix B.V. reinforces its commitment to international compliance standards and strengthens the security and transparency of its gaming platform against financial crime threats.

Factors considered to evaluate Delivery Channel Risk:

- Whether the Company with the client conducted on a non-face to face basis
- Whether the Company personally knows the customer and conducts business on face-to-face basis
- Client not known by the Company but well known in the industry and came to the Company by trusted sources

6.4 Technological Developments Risk Assessment

Prior to the launch of any new technology, digital product, delivery method, or operational process, Geosix B.V. conducts a formal and documented technological risk assessment. This process is mandatory and forms a core component of the Company's risk-based approach to AML/CTF/CPF compliance.

The risk assessment must be:

- Completed and reviewed prior to deployment, ensuring no new technology is introduced without first understanding its vulnerabilities and potential misuse.
- Fully documented in writing, including details of the product or system being assessed, identified risks, mitigation measures, residual risk levels, and decision-making rationale.
- Retained in internal compliance records and made available to the Curaçao Gaming Control Board (GCB) upon request.

Documented assessments are required for:

- New gaming platforms, digital tools, or payment channels.
- Any update to existing infrastructure that significantly changes risk exposure.
- The use or integration of AI systems, blockchain, or third-party services.
- Innovations involving anonymous payment mechanisms or remote account access.

This approach ensures all technological advancements are introduced responsibly, with due consideration for AML/CTF/CPF risks and are aligned with the supervisory expectations of the GCB.

Geosix B.V. is dedicated to ensuring that advancements in technology are not exploited for the purpose of financial crimes such as money laundering (ML) or terrorist financing (TF). As innovation continues to transform the iGaming sector, the company implements robust controls and a proactive risk management framework to identify and mitigate any vulnerabilities associated with technological change. Through the integration of thorough

risk evaluation processes, Geosix B.V. safeguards its compliance obligations across all new business practices, service models, and product innovations.

Procedures for Risk Identification and Assessment

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

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

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

6.5 Implementation of Risk Mitigation Strategies

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

- **Strengthening of Security Protocols** – The implementation of multi-factor authentication (MFA), biometric identity verification, end-to-end data encryption, and artificial intelligence (AI)-based fraud detection tools to safeguard systems from misuse;
- **Enhancement of Transaction Monitoring Capabilities** – Upgrading monitoring platforms to detect atypical financial behavior using automated systems capable of flagging transaction patterns indicative of ML or TF;
- **Policy Adaptation** – Revising AML/CTF policies to address new risk factors introduced by evolving technology. The company ensures that its compliance framework remains agile, keeping pace with the dynamic nature of cybercrime and financial crime techniques.

Through ongoing monitoring and adjustment to technological developments, Geosix B.V. upholds its commitment to maintaining a secure and compliant operational environment. This forward-looking strategy protects the integrity of the company's financial ecosystem and affirms its alignment with global AML/CTF obligations. By doing so, the company

ensures that innovation is not pursued at the expense of regulatory compliance or financial security.

Based on the analysis of the risk indicators, the risk model calculates a risk rating of low, medium or high which is then used to create a risk profile which is then assigned to the players and payment service providers at the onboarding stage and is reassessed and amended during the business relationship within the framework of periodic KYC/KYB reviews. Online casinos possess inherent high risks, so the Company strives to rely on its AML and Anti-Fraud key personnel to maintain effective internal controls and CDD measures as reflected in relevant policies.

6.6 Sector-Specific Risks in iGaming

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, or deposit/withdraw avoiding customer due diligence (CDD) measures.
- Multiple Casino Accounts: Usage of several accounts to mask gambling activities.
- Anonymous Customers: Individuals redeeming substantial amounts 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);
- 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, 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, 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 no4. 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 assesses 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.

7. Client Due Diligence Guidelines and Acceptance Policy

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.

In the context of AML, client due diligence process is a procedure which includes the identification of the potential client, verification of his/her identity and age, collection of additional information to construct an economic profile of the account holder, assign a risk rating, and monitor his/her behavioral and transactional patterns for any deviations that may be construed as a violation of AML/CFT legislation and policies. Research into the clients can be done via open- source tools such as social media checks, property ownership checks, employment checks, insolvency checks etc. Due Diligence measures may be simplified when the analysis of the initial client data places such applications in a low-risk category, whereas Enhanced Due Diligence (EDD) is applied to cases that require additional screening due to the system flagging certain data entries such as PEPs (politically-exposed persons), clients from high-risk jurisdictions etc .

Geosix B.V. has developed a comprehensive risk-scoring framework that classifies clients according to predefined risk profiles derived from factors such as their geographic location, transactional patterns, and the products they utilize. The integrity of **Geosix B.V** gaming environment is safeguarded through the implementation of advanced protocols that integrate modern technologies and third-party databases. These include a proprietary anti-fraud system for onboarding and transaction monitoring, artificial intelligence (AI) tools, biometric identification where applicable, and RegTech screening solutions.

The company remains committed to complying with regulatory requirements that prohibit the creation of anonymous or fictitious accounts within the gaming sector. To effectively

mitigate risks associated with money laundering, terrorist financing, and proliferation, the verification of player identities and a clear understanding of their business relationships are essential. A robust Client Due Diligence (CDD) policy serves as the foundation for assessing risk and ensuring full adherence to regulatory obligations. Any activity identified as suspicious will be reported to the Financial Intelligence Unit (FIU) and, when required, to the Public Prosecutor's Office.

A Client Acceptance Policy (CAP) has been established to categorize players into low, medium, and high-risk profiles based on geographical location, transaction behavior, income source, and other factors. The CAP outlines enhanced due diligence measures and specifies scenarios where services will be denied due to elevated ML/TF risk. For more detailed information please refer to the **Appendix IV (Client Acceptance Policy)**.

7.1 The company applies CDD measures

In addition, the Company recognizes the relevance of Articles 2–4 of the National Ordinance Penalization of Money Laundering (NOPML), which define money laundering and related criminal acts, thereby forming the legal basis for identifying suspicious activity during the CDD process. The Company also implements controls to detect conduct that constitutes aiding, facilitating, or failing to prevent money laundering or terrorist financing, which are criminalized under Articles 6–7 NOPML.

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.

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

- Full name

- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number
- For low-risk scenarios, only basic information will be required. In higher-risk situations, more detailed information will be collected to mitigate the risks associated with money laundering and terrorist financing.
- Risk Evaluation: Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.
- Verification Methods: Identity verification will be executed through:
 - Government-issued photo identification (e.g., passport or ID card).
 - Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.
 - Verification of the address through communication methods such as letters, email, or phone.
 - Biometric checks, cross-referencing database information, IP addresses, and funding methods.
- If initial information is insufficient, further verification steps may include requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

The company will seek to identify the purpose and nature of its relationships with players as part of the CDD process. While some relationships may be clear, the company will gather sufficient information to detect any unusual or suspicious activities. For higher risk

clients, detailed documentation of their source of wealth and expected activity levels will be collected to ensure legitimacy. For lower and medium-risk players, basic employment or business information will suffice, supplemented by independent verification for higher-risk individuals.

7.3 Timing of Client Due Diligence Measures

Geosix B.V enforces the timely implementation of Client Due Diligence (CDD) procedures to ensure full compliance with applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These procedures are designed to proactively identify and verify clients in accordance with regulatory requirements and internal risk assessments.

CDD Triggered by Transaction Thresholds

At the point of account registration, **Geosix B.V** collects and verifies core client information, including full legal name, permanent residential address, and date of birth. Additionally, clients undergo Politically Exposed Person (PEP) screening and are cross-checked against relevant sanctions lists to ensure they are not linked to prohibited or high-risk entities.

In line with the company's risk-based approach, full identity verification is completed prior to processing any financial transaction that reaches or exceeds the threshold of NAF 4,000. This requirement applies to both individual transactions and cumulative transactions such as multiple deposits, withdrawals, or player-to-player transfers that collectively meet the threshold within a relevant time frame.

Geosix B.V actively monitors all financial activity on a continuous basis. Transaction data is aggregated daily to ensure that the cumulative behavior of each player is considered when assessing risk exposure and determining the need for additional due diligence.

When the threshold of NAF 4,000 is met, the company conducts a comprehensive client risk assessment. This includes reviewing all previously collected information, completing any outstanding CDD obligations, and updating the client's risk classification as needed.

Early Execution of CDD Procedures

As a proactive measure, Geosix B.V. aims to complete CDD procedures at the earliest opportunity preferably during account registration regardless of whether a financial threshold has been reached. By verifying client identities prior to their participation in financial transactions, the company reduces the likelihood of criminal actors exploiting the platform before thorough due diligence has been conducted

Temporary Restrictions for Incomplete CDD

In circumstances where a client reaches the NAF 4,000 threshold before completing full CDD verification, Geosix B.V. applies specific transactional restrictions to preserve regulatory compliance:

If the threshold is met due to a deposit, the client is prevented from making further deposits or withdrawals. However, they may continue using existing funds for gameplay activities.

If the threshold is reached due to a withdrawal request, the client's account is temporarily frozen, and all gaming activity is suspended until the verification process has been finalized.

Handling Non-Compliance with CDD Requirements

If a client fails to submit the required CDD documentation within 30 days of reaching the NAF 4,000 threshold, Geosix B.V. initiates corrective action. The business relationship is terminated, and depending on the circumstances, the company takes the following steps:

If the situation gives rise to a reasonable suspicion of ML or TF, a Suspicious Transaction Report (STR) is submitted to the Financial Intelligence Unit (FIU).

In the absence of such suspicion, the remaining funds are returned to the original deposit source (e.g., the client's verified bank account or digital wallet).

If there are lingering concerns about possible financial crime, the company evaluates whether the funds should be frozen in accordance with its internal escalation procedures and regulatory requirements.

Managing Tipping-Off Risks

Geosix B.V. is mindful of the risks associated with tipping off a client during account restriction or closure. In such cases, the company ensures that all actions are carried out discreetly and in accordance with legal obligations. Staff are guided by internal procedures designed to avoid breaching anti-tipping-off provisions while maintaining full regulatory compliance.

By ensuring that CDD measures are implemented swiftly and in alignment with financial activity thresholds, Geosix B.V. strengthens its defences against financial crime, upholds transparency, and safeguards the integrity of its gaming platform across all operational channels.

Continuous Surveillance of Existing Clients

Geosix B.V. applies Client Due Diligence (CDD) not only at the onboarding stage but also throughout the duration of the client relationship. The company is committed to maintaining a high standard of compliance by performing ongoing monitoring and routine reassessments, ensuring that all client activity remains consistent with prevailing Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations.

7.4 Ongoing Review and Risk-Based Monitoring

Client relationships are subject to continuous due diligence measures. This includes the regular monitoring of transactions and the reassessment of client risk profiles in light of new behaviors or patterns. Where necessary, the company re-evaluates previously collected data to ensure it remains accurate, complete, and relevant. Any deviation from expected conduct prompts further review and, where applicable, the application of enhanced scrutiny.

For clients who were previously onboarded with limited or incomplete CDD, Geosix B.V. initiates retrospective due diligence procedures. These are prioritized based on risk, with high-risk clients undergoing immediate verification. Periodic updates are also conducted in accordance with both internal policies and regulatory guidance to ensure that CDD measures remain aligned with risk exposure and evolving compliance standards.

Reapplication of CDD Based on Risk Triggers

Geosix B.V. applies full CDD measures to existing clients under specific conditions that indicate increased risk or regulatory necessity. These conditions include, but are not limited to:

A material change in the client's behavior or risk profile, such as sudden high-value transactions, relocation to a higher-risk jurisdiction, or being identified as a Politically Exposed Person (PEP).

Legislative or regulatory amendments that require updated or additional client verification.

The client engaging in one or more transactions totalling NAF 4,000 or more, which automatically triggers full identity verification and documentation review under the company's CDD policy.

Remediating Gaps in Historical CDD

In instances where clients were previously allowed to transact without complete CDD such as during legacy onboarding procedures or prior to the implementation of current regulatory standards Geosix B.V. takes corrective action. High-risk clients are prioritized for immediate verification, while others are subject to a scheduled review based on the level of risk they present.

CDD is applied using a proportional and risk-sensitive approach, ensuring that resources are allocated where they are most needed and that lower-risk clients are still monitored effectively. Verification processes may include updated identity checks, refreshed PEP and sanctions screenings, and a reassessment of the client's source of funds and wealth.

By extending due diligence practices beyond initial onboarding and embedding them into the ongoing management of client relationships, Geosix B.V. strengthens its regulatory compliance, reduces its exposure to financial crime, and upholds the integrity of its platform across all client segments.

7.5 Termination of Business Relationships

Geosix B.V. maintains the right to terminate business relationships with clients who fail to comply with Client Due Diligence (CDD) requirements or who present heightened financial crime risks. This measure ensures the company's adherence to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations while preserving the security and integrity of its operations.

Business relationships are subject to termination when a client engages in suspicious or unexplained financial activities, fails to submit required CDD documentation within the prescribed timeframe, or is determined to pose a significant risk of involvement in money laundering or terrorist financing. The decision to terminate a relationship is subject to formal internal review and must be approved by senior management.

Prior to termination, a final review of the client's account activity is conducted to identify any outstanding irregularities. If any transaction raises suspicion of ML, TF, or PF Geosix B.V. submits a Suspicious Transaction Report (STR) to the Financial Intelligence Unit (FIU) without delay. All records associated with the terminated relationship are retained securely for a minimum of five years in accordance with regulatory requirements. This approach reinforces the company's commitment to proactive risk management and ensures regulatory compliance through the entire client lifecycle.

Where risk cannot be adequately mitigated such as uncooperative clients, unresolved discrepancies, or confirmed links to sanctioned entities Geosix B.V. will terminate the business relationship and report such instances to the Financial Intelligence Unit (FIU)

7.6 Third-Party Reliance for Client Due Diligence

Geosix B.V. may, under controlled circumstances, rely on qualified third parties to carry out specific components of the Client Due Diligence (CDD) process. Such reliance is implemented strictly within the boundaries of applicable AML/CTF/CPF laws and does not absolve the company of its legal responsibility to ensure full compliance. **Geosix B.V.** remains ultimately accountable for the accuracy, completeness, and timeliness of all CDD-related activities performed on its behalf.

When relying on a third party, the company ensures that all relevant client identification and verification information is accessible without delay upon request. Third-party arrangements are governed by formal agreements that clearly outline data-sharing protocols, compliance obligations, and procedures for independent compliance audits. These agreements require the third party to be a regulated entity subject to robust AML/CFT supervision and to maintain an independent relationship with the client.

Importantly, **Geosix B.V.** differentiates between third-party reliance and outsourcing. In a reliance scenario, the external party performs selected CDD tasks independently, while **Geosix B.V.** retains full responsibility for assessing client risk, verifying Politically Exposed Person (PEP) status, and maintaining ongoing transaction monitoring. In an outsourcing arrangement, the third party operates under **Geosix B.V.'s** direct oversight, following its internal policies and regulatory framework.

Before engaging with any third-party service provider, **Geosix B.V.** conducts a comprehensive risk assessment of the provider's jurisdiction, evaluating its regulatory environment and compliance history. This is supported by intelligence from international

watchdogs and enforcement bodies. Regular assessments both quantitative and qualitative are performed to monitor the third party's performance and ensure the effectiveness of their procedures. These reviews verify that decisions regarding business relationships and risk classification remain under the exclusive control of **Geosix B.V.**

Through structured oversight and stringent regulatory controls, **Geosix B.V.** ensures that any third-party involvement in CDD processes contributes to a secure, transparent, and compliant operational environment.

7.7 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.

To meet this obligation, **Geosix B.V.** applies with the following measures:

- Identify and verify natural persons who ultimately own or control 25% or more of the equity, voting rights, or capital of a legal entity, whether directly or indirectly.
- Where no individual meets the ownership threshold, identify any persons who otherwise exercise effective control, such as through:
 - Voting arrangements, contractual relationships, or positions of influence (e.g., board control or management power).
 - Indirect control mechanisms, such as trusts, nominee arrangements, bearer shares, or layered ownership through multiple legal entities.
- Conduct multi-tiered analysis in cases where ownership is obscured through multiple corporate layers or complex holding structures, to trace and identify the natural person(s) exercising ultimate control.
- Obtain and review reliable documentation such as:
 - Shareholder registries, articles of incorporation, beneficial ownership registers.
 - Declarations from legal representatives clarifying control and ownership hierarchy.
 - Organizational charts and financial disclosures when necessary.
- Where no individual qualifies under the above, identify the most senior managing official as a fallback UBO, in accordance with the “last resort” principle under FATF and CGA guidance.
- Verify beneficial ownership and control details using independent and reliable sources, and ensure this information is:
 - Accurately recorded and readily available for competent authorities.
 - Regularly reviewed and updated, particularly when:
 - There is a change in ownership or control.
 - The customer’s risk profile changes.
 - Trigger events occur (e.g., threshold transactions, suspicious activity).

Geosix B.V. does not enter or continue business relationships with legal entities whose beneficial ownership or control structures are non-transparent, unverifiable, or otherwise obstructive to due diligence.

8. Transaction 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 maintains 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.

In a nutshell, the Curacao regulatory landscape focuses on defining the indicators that may suggest the transaction is of an unusual nature so that it may be reported to the Curacao Financial Intelligence Unit (FIU Curacao). Therefore, an adequate transaction monitoring system is a vital part of complying with the licensing requirements in Curacao.

Geosix B.V.'s anti-fraud team is in charge of operating a proprietary anti-fraud system which analyzes players' data on the basis of the automatic checks performed through a number of electronic systems such as WorldCheck and manual checks performed by a team of analysts via various data sources. Any discrepancies identified by the first line of defense are escalated to the team lead and then may be ultimately reported to the AML/CFT Officer in writing through an internal suspicious activity report (SAR).

This system is an automated monitoring system which allows to monitor transactions in real-time, flagging suspicious activities based on predefined rules and thresholds. The anti-fraud team uses machine learning and data analytics to enhance detection capabilities and reduce false positives. Additionally, the system is configured in a such a way as to focus on high-risk transactions, such as large deposits, frequent transfers, and cross-border transactions and the parameters reflect current and emerging threats to capture bad actors by flagging suspicious activity internally, and, where necessary, to financial intelligence units (FIUs).

8.1 Transaction monitoring system

Automated System:

Advanced software solutions are utilized to conduct real-time transaction monitoring. These systems apply algorithms and machine-learning models to detect patterns or irregularities that may signal potentially suspicious activity.

Risk Assessment:

Clients and their transactions are evaluated based on multiple risk indicators, such as transaction volume and frequency, geographic location, and overall behavioral patterns.

Alert Generation:

When the system identifies conduct that meets predefined risk rules or exceeds threshold limits—such as unusually large transactions or repeated deposits and withdrawals—it automatically generates alerts. These alerts are subsequently reviewed by the Compliance Officer.

Common analytical techniques include geolocation tracking, source-of-funds verification for high-value transactions, behavioral analysis to identify deviations from a client's typical betting or gambling habits, and transaction-velocity checks, such as rapid movement of funds or frequent high-value transactions within short timeframes.

CDD Triggers:

Client Due Diligence (CDD) is initiated under the following circumstances:

Creation of an online account

Doubts regarding the authenticity or accuracy of submitted information or documents
Suspicious client profile or transactional behavior

Unauthorized attempts to alter a player's profile

A single transaction, or a series of linked transactions, totaling 4,000 NAF or more

When transactions meet or exceed the 4,000 NAF threshold (or equivalent in another currency), CDD measures are automatically applied. For these purposes, a "transaction" includes placing a wager, depositing funds, or withdrawing winnings. Periodic reviews of existing records and ongoing monitoring of players' transactional patterns are also integral components of the CDD framework.

To combat money laundering, fraud, and terrorist financing, players' IP addresses are monitored through tools embedded within the proprietary anti-fraud system. This ensures platform access only from non-restricted jurisdictions and helps identify red flags such as multiple accounts created by the same individual, access attempts by blacklisted or self-excluded persons, or other forms of suspicious conduct. The proprietary software additionally tracks player data including transaction history, wager amounts, win/loss information, geolocation, gambling patterns, and session durations. These monitoring tools are particularly important when a client's risk rating is elevated due to behavioral or transactional indicators suggesting potential AML/CFT concerns.

If CDD measures cannot be completed, the account is locked during the verification process, and ultimately the business relationship is terminated for failing to meet AML/CFT requirements. In such cases, funds are returned to the client via the same payment method and originating account used for the deposit.

9. Politically- Exposed Persons (PEPs)

Enhanced Due Diligence (EDD) is a crucial process in the online betting and gambling industries aimed at preventing money laundering, fraud, and other illicit activities. EDD refers to the additional measures taken by companies to thoroughly verify the identity and background of their clients, particularly those posing higher risks. High-risk clients in the online gambling and betting setting are those who have high transaction volumes, deposit or withdraw large amounts, exhibit unusual betting patterns or are Politically Exposed Persons (PEPs). A PEP is an individual who recently held or is currently holding a prominent public position such as a head of state, member of the Parliament, government, directors of international organizations etc. Family members of PEPs and close associates are also considered PEPs, so their applications are also treated as high-risk by the Anti-

Fraud team and relevant risk management procedures are activated when processing such requests through the senior management.

At **Geosix B.V.** PEPs' cases are handled by the senior management team whose approval is necessary to transact with such individuals. Furthermore, an internal register of such cases is kept by the Compliance Officer.

10. Sanctions Management, FATF High-Risk List, License Restrictions

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.

All updates are reflected promptly in internal systems. Detailed Sanction Policy is described in **Appendix III**.

Update Mechanism and Frequency

Sanctions lists are updated at least daily and immediately upon publication of new updates by the competent authorities. Geosix B.V. uses automated sanctions-screening tools that synchronize with official sources in real time to ensure that the most current sanctions information is applied. In addition, the Compliance Officer conducts a minimum monthly review of any amendments or circulars published by the Curaçao Gaming Control Board or relevant government authorities to confirm alignment with local obligations.

Responsibilities

The Compliance Officer (or Sanctions Officer, where designated) is responsible for ensuring that sanctions lists are up to date, verifying tool synchronization, reviewing any alerts or potential matches, escalating confirmed matches, and ensuring adherence to regulatory requirements.

All sanctions-screening results, update logs, alerts, and match decisions are documented and retained for a minimum of five (5) years in accordance with applicable AML/CFT and sanctions regulations.

11. Suspicious Activity Reporting

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.

Deposits in the amount of NAF. 5,000 or more.

Withdrawal in the amount of NAF. 5,000 or more

According to article 1 of 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 client is to be paused or terminated, depending on the circumstances.

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.

Suspicious activity may include using several anonymous payment methods

i.e. prepaid cards; location of the payment method does not correspond to the geolocation of the client; depositing a large sum and withdrawing it after no gaming or little gaming activity; a withdrawal request to a third-party payment method.

Suspicious activity may include using an intermediary for document-related requests; source of wealth does not match the reported financial data; frequent changes of ownership in a short time; lack of willingness to provide due diligence documentation.

Geosix B.V. keeps detailed records of all transactions and activities that seem suspicious, including dates, amounts, methods, and any other relevant details. As regards clients, the anti-fraud and AML teams document all available information about the individuals or entities involved, including names, addresses, account numbers, and identification.

11.1 Objective and Subjective Indicators (NORUT Compliance)

The Company fully incorporates the objective and subjective indicators as mandated under the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the applicable Ministerial Indicator Decree. These indicators form the legal basis for determining when a transaction must be classified as an *Unusual Transaction* and subsequently reported to the FIU Curacao.

- **Objective indicators:** Indicators where reporting is mandatory due to the transaction meeting a predefined condition (e.g., transactions involving sanctioned countries, specific transaction types, or legally defined thresholds).
- **Subjective indicators:** Indicators where the Company "knows" or "suspects"—or has reasonable grounds to suspect—that a transaction may involve money laundering, terrorist financing, proliferation financing, or related criminal activity.

All staff must be familiar with, and must apply, both sets of indicators when assessing client behaviour or transactional activity. Internal training ensures that employees understand how to identify and escalate indicators in accordance with the Indicator Decree.

11.2 Integration of FIU Ministerial Indicator Decree

The Company explicitly adopts and incorporates the Ministerial Decree Establishing Reporting Indicators issued under NORUT. The Company ensures:

- all objective and subjective indicators are continuously applied;
- employees are trained in their recognition;
- monitoring systems are calibrated to detect activities meeting these indicators;
- compliance procedures reflect the latest published indicator lists;
- periodic reviews are conducted to ensure alignment with updates issued by FIU Curaçao or the Ministry of Finance.

No internal interpretation may override an objective indicator—reporting is mandatory when such indicators apply.

11.3 Reporting Unusual Transactions “Without Delay”

In accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is legally required to report all Unusual Transactions (UTRs) to FIU Curacao “without delay” as per requirement in Art. 30(2) of the 2025 Regulations and Art. 8 NORUT.

To operationalize this legal requirement, the Company establishes the following internal reporting timelines:

- Immediate escalation from staff to Compliance Officer: *within 24 hours* of detection.
- Internal review and validation by Compliance Officer: *within 48 hours*.
- Submission to FIU Curaçao: *no later than 24 hours after validation*, and always without delay, in line with NORUT requirements.

Under no circumstances may the client be informed that an Unusual Transaction Report (UTR) has been filed (“tipping-off”).

11.4 Identifying Unusual Transactions

The Company recognizes that its obligations to identify, classify, and report Unusual Transactions are established under Articles 3–8 of NORUT, which impose mandatory duties relating to the submission of Unusual Transaction Reports (UTRs) to FIU Curaçao. The Company also acknowledges the requirement under Article 10 NORUT to apply both

objective and subjective indicators, as defined in the Ministerial Indicator Decree (NORUT). Objective indicators trigger automatic reporting without discretion, while subjective indicators impose a duty to report when suspicion or reasonable grounds to suspect criminal activity exist.

Geosix B.V. defines an unusual transaction as any financial activity that deviates materially from a client's established behaviour or declared financial profile. These may include large or unexpected money movements, transactions involving unknown or unverified third parties, or financial activity lacking a clear legal or economic purpose.

The company relies on advanced transaction monitoring systems to detect such anomalies. When flagged, these transactions are forwarded to the Compliance Officer for deeper review. Staff members are trained to recognize behavioral and transactional red flags and to act promptly in escalating concerns.

The following categories of transactions are considered particularly noteworthy and may trigger further examination or reporting:

Previously Reported Activities: Transactions already identified and forwarded to judicial or law enforcement agencies such as the police or public prosecutor for potential links to ML or TF are automatically categorized as unusual.

Dealings with Sanctioned Persons or Entities: Any transaction involving a party listed under the Sanctions National Ordinance (N.G. 2014 no. 55), or other relevant sanction regimes, is flagged and treated as unusual.

High-Value Transactions: Transactions equal to or exceeding NAF 5,000 regardless of the method of payment are subject to scrutiny. This includes:

Deposits or withdrawals at or above the threshold.

Purchases of gaming tokens, digital credits exceeding the limit.

Redemptions or payouts of winnings at or above the specified amount.

The threshold also applies to a series of transactions that cumulatively total NAF 5,000 or more within a single gaming day. Such cumulative activity is evaluated in aggregate when determining whether reporting is necessary.

In cases where there is a reasonable basis to suspect that a transaction is connected to ML, TF, or PF whether due to the nature of the transaction, the behavior of the client, or other risk indicators it must be treated as suspicious and subject to internal escalation procedures.

Timely Reporting to the FIU

Once a transaction is determined to be unusual or suspicious, **Geosix B.V.** is obligated to file a report with the Financial Intelligence Unit (FIU) without delay, in accordance with AML Regulation IV.1 and reporting requirement under Article 30(2) of the January 2025 AML/CFT/CPF Regulations, reinforced by Article 8 NORUT, ensuring that all internal alerts, investigations, and external filings occur promptly and in accordance with the statutory

timeline. This requirement applies whether the transaction has been completed or merely attempted. The Compliance Officer is responsible for submitting the Unusual Transaction Report (UTR) immediately after the suspicion is confirmed, without waiting for additional approvals or administrative processes.

Confidentiality in Reporting

Maintaining strict confidentiality around Suspicious Activity Reports (SARs) is fundamental to preserving the effectiveness of the company's compliance regime and fulfilling its legal obligations. Employees are strictly prohibited from disclosing any details of a SAR to the person under review or to any unauthorized third party. Breaches of this confidentiality can undermine investigations, result in regulatory violations, and constitute a tipping-off offence under applicable legislation.

Only authorized personnel such as the Compliance Officer and designated members of the compliance team may handle SAR-related information. All such communications must be treated with the highest level of discretion. **Geosix B.V.** provides regular training to ensure staff understand the importance of maintaining confidentiality in all aspects of the reporting process.

Violations of this confidentiality policy are treated as serious compliance breaches and may lead to disciplinary action, including termination of employment. These protocols are critical to maintaining the integrity of the reporting framework and the company's ability to respond effectively to financial crime risks.

By fostering a culture of awareness, discretion, and accountability, **Geosix B.V.** strengthens its ability to identify suspicious behavior, uphold its obligations under AML/CTF/CPF regulations, and support broader efforts to prevent financial crimes across the iGaming sector.

12. 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 independence and authority of the role. The selected Compliance possesses relevant experience and expertise in AML compliance and is 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.

The Board ensures the Compliance Officer is adequately resourced, empowered, and supported in executing the AML/CTF/CPF program in accordance with Regulation V.3 of the CGA AML Guidelines. This structure safeguards the autonomy of the compliance function and ensures timely escalation of significant risks or breaches to the highest level of governance.

Responsibilities

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

- **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.
- **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.
- **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.
- **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.
- **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.
- **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.

13. 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.

GCB Supervision and Enforcement

The Company operates under the direct supervision of the Curaçao Gaming Control Board (GCB), as established in Article 4(1) LOK, which serves as the competent AML/CFT/CPF supervisor for the gaming sector. which designates the GCB as the competent authority responsible for AML/CFT/CPF supervision of licensed gaming operators.

Pursuant to its statutory mandate under Articles 5–9 LOK, the GCB is empowered to:

- Conduct on-site and off-site AML/CFT/CPF examinations (Art. 7 LOK);
- Request and obtain unrestricted access to documents, systems, data, and personnel (Art. 8 LOK);
- Assess the implementation of operator obligations under the Regulations for the Combatting of Money Laundering, Terrorist Financing, and Proliferation Financing (effective 1 January 2025), issued under Art. 11 LOK;
- Issue binding directives, mandatory remediation instructions, or improvement plans (Art. 9(1)(b) LOK);

- Impose administrative sanctions, including fines, conditional measures, license restrictions, suspension, or revocation (Art. 15–18 LOK).

The Company acknowledges that the January 2025 AML/CFT/CPF Regulations have binding legal effect under Art. 11 LOK, and non-compliance constitutes a regulatory breach subject to GCB enforcement actions under Art. 15-18 LOK.

14. Employee Training and Screening Program

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/FP 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. Full Employee Screening Program **Appendix II**

1. Pre-Employment Screening

Before onboarding any new employee, especially those in sensitive, client-facing, or compliance-related roles, the company conducts thorough background checks, including:

- Verification of identity and right to work using government-issued documentation.
- Criminal background checks to detect any prior financial or integrity-related offenses.
- Employment and reference verification to confirm qualifications and experience.
- Sanctions and PEP screening, using independent screening tools and global watchlists.

Candidates failing to meet the company's integrity or risk criteria are not employed.

2. Ongoing Employee Screening

Geosix B.V. continues to assess employee suitability after hiring through:

- Annual rescreening of employees in AML/CTF-sensitive roles.
- Event-driven screening, such as when suspicious activity, misconduct, or role changes occur.
- Monitoring for changes in sanctions exposure, PEP status, or relevant legal/regulatory risks.

All employee screening records are retained securely and confidentially, in compliance with data protection laws, for a minimum of five (5) years.

3. Training and Awareness

Employees, particularly those involved in onboarding, account management, or transaction processing, receive annual AML/CTF training tailored to their roles. This training ensures staff understand:

- The company's AML/CTF/CPF obligations.
- How to identify unusual behavior, such as:
 - Large or inconsistent bets.
 - Suspicious patterns of deposits/withdrawals.
 - Anonymous or third-party payments.
- How and when to file a Suspicious Activity Report (SAR).
- The importance of confidentiality and client data protection.

Employees are made aware that failure to comply with AML/CTF obligations may lead to disciplinary, administrative, or criminal consequences.

15. Record- Keeping Procedure

The Company acknowledges that its recordkeeping obligations originate from Articles 3–8 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), which require the retention of customer identification data, transaction records, and internal reports for the legally mandated period. These obligations are further reinforced under Part IV, Articles 28–35 of the January 2025 AML/CFT/CPF Regulations, which prescribe the retention of CDD data, transactional information, monitoring records, internal audit findings, STR/UTR files, and training documentation.

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 competent domestic authorities when requested, in accordance with applicable legal requirements.

We maintain comprehensive records, which include client identification information, transaction details, suspicious activity reports (SARs), training logs, and audit records, all preserved for a minimum of five years.

- The company securely maintains detailed records, including:
- Client identification information.
- Transaction histories.
- Suspicious activity reports (SARs).
- Staff training logs.
- Audit records.

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

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

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

16. AML/CFT/CPF Audit

In adherence to the new Curacao gaming legislation and Section V.5 of the Curaçao Gaming Authority's AML Guidelines, 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 in line with the expectations of CGA AML Regulation Section V.7 to ensure, if required, that corrective actions are taken and will monitor compliance to prevent future violations.

Geosix B.V. maintains an audit trail and full documentation of all internal audit activities for a minimum of five (5) years and makes such records immediately available to the Curaçao Gaming Control Board (GCB) upon request. The Company is committed to transparency, accountability, and continuous improvement in its AML/CTF/CPF compliance framework.

17. Regulatory Access and Legal Force

The Company confirms that it is subject to the supervisory and enforcement powers granted to the Curaçao Gaming Control Board (GCB) under the National Ordinance on the Supervision and Regulation of the Gaming Sector (LOK). Under Article 9 LOK, all supervisory instructions, directives, and remedial measures issued by the GCB are legally binding and enforceable.

The Company further acknowledges that the development and implementation of its internal systems, controls, monitoring mechanisms, and reporting processes are designed to fully comply with:

- Part II (Articles 3–13) of the January 2025 AML/CFT/CPF Regulations (governance,

risk management, internal controls);

- Part III (Articles 14–27) (CDD, EDD, ongoing monitoring);
- Part IV (Articles 28–35) (recordkeeping, reporting, internal audit, employee training).

The Company commits to full cooperation with the GCB during all supervisory examinations, information requests, and enforcement processes pursuant to Articles 5–9 LOK.

Geosix B.V. fully acknowledges the supervisory and enforcement authority of the Curaçao Gaming Control Board (GCB) as prescribed in Section V.6 of the GCB AML Guidelines and commits to complete, proactive cooperation with all regulatory examinations and oversight activities. To this end, the company grants the GCB and any other legally empowered authority unrestricted, immediate, and comprehensive access to all data, systems, records, and personnel necessary for the assessment of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework.

This includes, but is not limited to:

- Customer due diligence records
- Transaction histories and monitoring data
- Internal risk assessments
- Policies and procedures
- Communication logs and training materials
- Audit trails, reports, and logs
- Compliance-related systems and platforms

Access shall be granted for both on-site and remote inspections, including the right to request supplementary documentation, system walkthroughs, and clarifications. Geosix B.V. ensures that all required information is readily retrievable, promptly provided upon request, and securely maintained for a minimum of five (5) years, or longer where legally mandated. Furthermore, the company commits to full cooperation with any post-inspection findings, including corrective action plans and remedial steps as directed by the GCB.

Binding Legal Effect

The Company acknowledges that as of **January 2025**, all provisions of the AML/CFT/CPF Regulations carry binding legal effect pursuant to the National Ordinance on the Supervision and Regulation of the Gaming Sector (LOK) and related AML/CFT legislation including NOIS, NORUT, NOPML, and the Sanctions National Ordinance (SNO). Failure to comply may result in administrative sanctions, mandatory remediation, license restriction, suspension, or revocation.

The Company ensures that all employees and management are aware of the binding nature of these Regulations and that all internal controls are designed to fully comply with these requirements.

18. Appendixes

Appendix I

Player Risk Scoring Assessment

Client no.:		Name:	

HOW TO USE THIS?	
1. Only yellow and blue fields have to be filled.	
2. Comment section is available, however, it is not necessary for calculation of risk level.	
3. Majority of questions has dropdown list or checkbox. Correct answer(s) should be selected.	

NEW total score:	0.00
NEW risk level:	Low
Onboarding specialist:	
Last update date:	

Category	Score
low	1-1.5
medium	1.5-2.4
high	2.4 or more
unacceptable	

Risk Category	Question	Risk score	Risk level	Additional comments
Client	Customer's Age			
Geography	Customer's Citizenship			
Geography	Customer's Second Citizenship			
Geography	Customer's Country of Birth			
Geography	Customer's Country of Residence			
Client	Does Customer have the status of PEP/IRCA (Politically Exposed Person/Relative and Close Associate)?			
ACCOUNT PROFILE				
Client	Purpose of account registration?			
Client				
Client				
FUND SOURCE AND INCOME STATUS				
Client	Source of funds	average		
Client				
Client				
Client				
Client				
Client	Source of wealth	average		
Client				
Client				
Client				
Client				
INTENDED ACCOUNT ACTIVITY (DEPOSITS)				
Transactions	Average frequency of transactions			
Transactions	Expected total value of transactions per period (NAF)			
Transactions	Types of incoming payments	average		
Transactions				

Risk Category:	To be:	Sum:	Weight:
Client	20%	0	
Geography	20%	0	
Products and Services	20%	0	
Transactions	20%	0	
Channels	15%	0	
Other	5%	0	
		0	

Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
INTENDED ACCOUNT ACTIVITY (OUTGOING PAYMENTS)				
Transactions	Average frequency of transactions			
Transactions	Expected total value of transactions per period (NAF)			
Transactions	Types of outgoing payments	average		
Transactions				
Transactions				
Transactions				
Transactions				
Transactions	Reasons for outgoing payments	average		
Transactions				
Transactions				
Transactions				
GAMING BEHAVIOUR				
Products and Services	Please indicate services of interest	average		
Products and Services				
Products and Services				
Products and Services				
Products and Services				
CONFIRMATIONS				
Payment Channels	Channels	average		
Third-party involvement				
Access				
Onboarding				
Client	Adverse media level			
Other	Manual risk level adjustment based on the expert judgement (± 5):			Comment regarding manual risk adjustment: Summary of the applicant:

Appendix II

Employee Screening Program

This Employee Screening Program (“Program”) sets out the mandatory standards and procedures for the vetting, assessment, and ongoing monitoring of all individuals employed or otherwise engaged by Geosix B.V.

The Program is adopted in accordance with CGA AML Regulation V.4, which requires firms to maintain robust employee screening measures both prior to hiring and throughout the duration of employment.

An Employee Screening Checklist forms an integral part of this Program and must be completed in every case as documentary evidence that all required screening steps have been properly carried out.

This Program applies to:

- All full-time, part-time, temporary, and contracted employees;
- Senior Management, the Compliance Officer, and any employee involved in AML/CTF responsibilities;

- Individuals engaged through outsourced or third-party arrangements who perform regulated or sensitive functions.

No individual may begin work or assume duties in any sensitive role until all screening requirements set out in this Program have been fully and satisfactorily completed.

Requirements

Geosix B.V. must ensure that all individuals are fit, proper, and suitable to perform their assigned duties. All screening procedures must be risk-based, proportionate to the sensitivity of the role, and properly documented.

The screening framework consists of:

- (a) Pre-Employment Screening
- (b) Fit-and-Proper Assessment (for designated roles)
- (c) Ongoing Screening
- (d) Completion of the Employee Screening Checklist

Pre-Employment Screening

Human Resources (“HR”), together with the Compliance Department, shall perform the following mandatory checks before any employment offer is finalized:

- Criminal Background Checks

A criminal record certificate must be obtained to confirm that the applicant has not been involved in offenses related to dishonesty, fraud, financial crime, money laundering, terrorist financing, or any conduct inconsistent with the integrity expected of Company staff.

- Identity Verification

Applicants must provide valid, government-issued identification. HR is responsible for verifying both identity authenticity and accuracy.

- Verification of Academic and Professional Qualifications

All educational credentials, licenses, certifications, and other professional qualifications relevant to the position must be independently validated.

- Employment History Verification

The Company shall verify prior employment, duties performed, and general conduct, subject to applicable legal constraints.

- Reference Checks

A minimum of two professional references must be obtained and documented. Any adverse or inconsistent information must be escalated to the Compliance Department.

Completion of the Employee Screening Checklist is required before an employment offer can be finalized.

Fit-and-Proper Assessment

A formal Fit-and-Proper Assessment is required for designated roles to determine suitability and professional integrity. The assessment considers:

- Integrity and Reputation

Absence of regulatory actions, criminal convictions, ethical breaches, or behavior inconsistent with professional honesty.

- Competence and Capability

Relevant qualifications, AML/CTF knowledge, technical skill, and overall ability to fulfil regulatory and operational duties.

- Financial Soundness

Where legally permissible, assessment of financial history including bankruptcy, insolvency, or financial misconduct.

- Independence and Conflicts of Interest

Ability to perform the role free from actual or perceived conflicts.

A Fit-and-Proper Assessment Form must be completed, reviewed by Compliance, and retained with the Screening Checklist.

Ongoing Screening and Monitoring

Periodic Screening

Employees in sensitive, compliance-related, or high-risk roles shall undergo screening at least annually, including but not limited to:

- Updated criminal record checks (where legally permissible),
- Role suitability evaluations,
- Conduct and performance reviews,
- Confirmation of continued independence and absence of conflicts.

Trigger-Based Rescreening

Additional screening is required when:

- An employee is promoted or transferred to a sensitive role,
- Allegations or indicators of misconduct are identified,
- Regulatory or business changes increase the risk profile of the role,
- External information gives rise to concerns regarding fitness or propriety.

Continuous Conduct Monitoring

Supervisors and the Compliance Department must report any concerns regarding employee behavior or integrity for immediate assessment.

Mandatory Checklist Completion

For each periodic or trigger-based rescreening, the Employee Screening Checklist must be updated and retained.

Documentation and Record-Keeping

Geosix B.V. shall maintain complete and accurate records of all screening activities, including:

- Background and criminal check reports;

- Verification documents;
- Fit-and-Proper Assessments;
- Completed Screening Checklists;
- Internal approvals, decisions, and escalation notes;
- Any adverse findings and remediation steps.

All records must be kept for a minimum of five (5) years, or longer where required by law or regulation, and must be made available to competent authorities upon request.

Responsibilities

Human Resources

- Administers pre-employment screening and maintains screening files.
- Ensures completion of the Employee Screening Checklist.
- Escalates concerns to Compliance.

Compliance Officer

- Oversees screening for AML/CTF-related roles.
- Conducts Fit-and-Proper Assessments.
- Approves employment in sensitive roles.
- Ensures compliance with CGA Regulation V.4.

Senior Management

- Ensures adequate resources and oversight.
- Approves any exceptions or escalated cases.
- Reviews periodic compliance reports.

Compliance and Enforcement

Failure to comply with this Policy, including failure to complete the Employee Screening Checklist or Fit-and-Proper Assessment, may result in disciplinary action up to and including termination of employment.

The Company affirms that this Policy satisfies the requirements of CGA AML Regulation V.4 and shall review the Policy annually to ensure continued regulatory compliance.

New Employee check list

Copy of national identity card or passport

Valid work permit (if applicable)

Proof of residence (utility bill, rental contract, or government-issued document)

Certificate of clear criminal record

Reference letter from previous employer

Professional licenses and certificates (if relevant to the position)

Curriculum Vitae (CV)

Good Repute & Fit-and-Proper Questionnaire

Diploma or proof of higher education

AML/CFT Policy and Internal Operating Manual (IOM) Acknowledgement Letter

Privacy Notice Acknowledgement

Induction & Initial Training Policy Acknowledgement Form

Appendix III

Sanctions policy

Background

Geosix B.V. is obliged to comply with laws imposing financial and other restrictions on dealings with certain entities, individuals and countries. This Sanctions Policy (hereinafter the “Policy”) sets out requirements and procedures designed to promote compliance with such laws (sanctions). Sanctions are a policy tool that national governments and multinational organisations use to constrain and deter perceived threats to their security, or to conform international conduct to recognised international standards. Sanctions arise in response to the conduct of countries, geopolitical rivals or transnational actors or trends. While national-level and multilateral sanctions regimes vary in content, rules, and restrictions, and the substance and frequency of enforcement action, they tend to fall into one of the below categories:

Comprehensive sanctions. These sanctions target entire countries or geographic regions (e.g., the Crimea Region of the Ukraine) and prohibit most activity involving those countries or jurisdictions. Comprehensive sanctions aim to alter government behavior by imposing economy-wide costs, restricting access to arms and tools of internal repression, and restricting access to a wide range of goods and services.

Regime-based sanctions. These sanctions target current (or former) governments or regimes. They are not comprehensive: although they are associated with particular countries, they are primarily list-based, focused on officials involved in activity deemed to be a threat to national security, economy, or foreign policy and on their associates. These sanctions tend to be paired with limited export controls or embargoes and related financing prohibitions. Most regime-based sanctions aim to protect human rights, combat state-sponsored or grand-scale corruption, and support democratic processes, institutions, and the rule of law.

Sectoral sanctions. These sanctions target entities in a key sector or sectors of a country’s economy. Importantly, they may still allow for many ordinary business transactions with the country at issue, even with respect to the listed entities. The listed entities may not be themselves involved in targeted activity, but they may be identified due to their relationship to government decision-makers (to exert pressure on those decision-makers) or because of their importance to a country’s economy or future growth prospects.

Special debt and/or equity sanctions. These relatively complex prohibitions allow for the continuation of day-to-day business with targeted entities while restricting the

ability of targets to deal in new or new equity (valuable for, e.g., raising capital for long-term projects). These sanctions have generally been applied to entities within specific economic sectors (e.g., energy) but have also been applied to entities owned or controlled by a target government.

Conduct-based sanctions. These list-based sanctions, as described in an additional resource, are directed not at particular countries or governments but rather at anyone involved in defined types of malicious activity. Persons and entities can be designated for involvement in terrorism, proliferation of weapons of mass destruction, bribery/corruption, human rights violations, drug trafficking, organized crime, election interference, and cyber-enabled malicious activity. Conduct-based sanctions are meant to identify, disrupt, and deter sanctioned activities.

The key types of sanctions listed above may vary on the above characteristics even within a single category. Nor are these key types of sanctions mutually exclusive (e.g., regime-based sanctions may overlap with special debt and/or equity sanctions).

Sanctions Regimes

Due to the nature of the business of the Company, different regulatory regimes may have jurisdiction over its transactions, Clients, products and services. This section outlines the major sanctions regimes and the basis of their jurisdiction directly impacting the Company's operations.

The United Nations (UN)

Under Chapter VII of the UN Charter, The United Nations Security Council (UNSC) can take action to maintain or restore international peace and security. The UN sanctions are administered by sanctions committees associated with the Security Council and are complemented by Financial Action Task Force (FATF) Recommendations 6 and 7. UNSC resolutions are legally binding to the UN member states.

The Company complies with sanctions restrictions imposed by the UN across all its operations.

The European Union (EU)

Sanctions are one of the EU's tools to promote the objectives of the Common Foreign and Security Policy (CFSP): peace, democracy and the respect for the rule of law, human rights and international law. The EU implements all sanctions imposed by the UN. In addition, the EU may reinforce UN sanctions by applying stricter and additional measures. Where the EU deems it necessary, it may decide to impose autonomous sanctions.

EU restrictive measures only apply within the jurisdiction of the EU, that is: a) within EU territory, including its airspace; b) to EU nationals, whether or not they are in the EU; c) to companies and organisations incorporated under the law of a member state, whether or not they are in the EU. This also includes branches of EU companies in third countries; d) to any business done in whole or in part within the European Union; e) on board of aircrafts or

vessels under the jurisdiction of a member state.

The Company complies with sanctions restrictions imposed by the EU across all its operations.

The United Kingdom (UK)

The UK financial sanctions apply, inter alia: a) within the territory and territorial waters of the UK and to all UK persons, wherever they are in the world, b) to all individuals and legal entities who are within or undertake activities within the UK's territory, c) to all UK nationals and UK legal entities established under UK law, including their non-UK branches; they must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

The Company complies with sanctions restrictions imposed by the United Kingdom to the extent that such sanctions do not contradict the laws of the European Union.

The United States (US)

In terms of applicability, the US sanctions fall into two categories:

primary US sanctions applicable to US persons, including all US citizens and permanent resident aliens regardless of where they are located, all persons and entities within the US, all US- incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods to comply.

secondary US sanctions: when applied, potentially subject non-U.S. persons to sanctions even if they are conducting business entirely outside of the United States and there is no US nexus in a relationship or a transaction. A number of sanctions programmes administered by the Office of Foreign Assets Control (OFAC) of the Department of the Treasury include secondary sanctions, including but not limited to Russia, Iran, Hong Kong/China sanctions programmes.

To the extent that is permissible under the local laws and the EU laws and regulations, the Company complies with both primary and secondary sanctions restrictions imposed by the US. Where compliance with secondary US sanctions is not permissible, e.g., regulation (EC) No 2271/96 and Joint Action 96/668/CFSP of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (OJ L 309, 29.11.1996, pp. 1 and 7), the Compliance Officer must escalate the matter to the Director(s) and the Board of Directors as a whole.

Statement

Under this Sanctions Policy, the Company must:

- Where required by law, block accounts and other assets of sanctioned entities and individuals.

- In all other instances, prohibit or reject unlicensed trade and financial transactions with sanctioned jurisdictions, entities, and individuals.
- Exit relationships with Clients confirmed to be subject to sanctions, regardless of whether this is required by local law in the jurisdiction where the account or relationship is based. In the event that an exit is not permissible under local law, this should be escalated to the Director(s) and the Board of Directors as a whole.
- The Company must not knowingly engage in any transactions and/or business relationships structured to or aimed at the circumvention of applicable sanctions restrictions.

Failure to comply with this Policy may expose the Company to regulatory action or fines, civil or criminal liability as well as possible reputational damage.

Staff responsible for breaches of sanctions related laws and regulations may also be exposed to criminal liability or fines. Staff who fail to comply with this Policy may be subject to disciplinary action, including dismissal.

Roles and Responsibilities

The Board of Directors

The responsibilities of the Board of Directors with regard to the Company's Sanctions Policy shall include:

- Reviewing and approving this Policy as required.
- Ensures effective communication of the importance of sanctions compliance throughout the organisation.
- Provides oversight to ensure the AML/CTF and sanctions compliance function receives adequate support and resources at every organisational level and has sufficient authority and independence to effectively exercise its responsibilities.
- The Board receives and considers regular compliance reports presented by the Compliance Officer, covering both AML/CTF and sanctions compliance.
- Appointing a qualified Compliance Officer with overall responsibility for the proper application the sanctions policy and provides this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the Board and the business lines.

The Director(s)

The Director(s) shall receive and evaluate regular compliance reports provided by the Compliance Officer and, where required, authorize changes based on the Compliance Officer's recommendations.

The Director(s) will also receive reports on particularly significant changes that may present risk to the Company as well as conflict of law and make the final decision regarding other

sanctions-related issues escalated by the MLCO as required by this Policy.

The Compliance Officer

The responsibilities of the Compliance Officer with regard to the Company's Sanctions Policy shall include:

- undertaking sanctions risk analysis of alerted transactions and/or potential and existing Clients including assessment of documentary evidence provided by Clients;
- proposing any necessary amendments to this Sanctions Policy and submitting them to the Board for approval;
- ensuring that all relevant employees are periodically informed of any changes in sanctions legislation, policies and procedures, as well as current developments and changes in sanctions evasion activities particular to their jobs;
- reviewing Client identification information to ensure that all the necessary information has been obtained.

All Other Employees

All Company employees should maintain continual awareness of the risk that sanctioned parties/transactions pose to the Company and its Client base and must not allow the Company to be used as a conduit for sanctions evasion. To support this, all staff are required to:

- Comply with this Sanctions Policy, related procedures, and applicable sanctions laws and regulations.
- Remain alert and promptly report to the Compliance Officer possible sanctions violations, or Clients found to be engaging in sanctions evasion activities or violations of this Policy or related procedures.
- Refrain from providing advice or other assistance to individuals or entities who seek to violate or attempt to violate any sanctions law or regulation, this Policy, or related procedures.
- Complete all required sanctions compliance training in a timely manner.
- In discussion or correspondence with Clients, staff are strictly prohibited giving any form of advice which might be seen as helping Clients to structure transactions or accounts in a way which could constitute sanctions evasion.

Sanction Screening

The Company must ensure that sanctions screening is performed on existing and prospective Clients, connected parties, transactions and third parties against sanction lists.

The specialized third party risk management solution selected by the Company shall ensure ongoing sanction screening process after a business relationship is established. The

potentially matching data from various sanctions and watchlists is compared against the applicant profile to establish an exact match, before a match status is assigned. The following types of status may be assigned:

True positive: Applicant data exactly matches one or several watchlist records.

Potential match: Name of the applicant matches one or several watchlist records, but the age/year of birth data is missing, or the applicant is suspected of committing a crime.

False Positive: Applicant data does not match any of the watchlist records.

- Applicant data matches the watchlist record exactly, but additional information clearly shows that the applicant and the person on the record are different people.
- Applicant data matches the watchlist record, but the record does not include criminal or suspicious information about a person. For example, if the applicant is a crime journalist, and their name features on the article as the author.

Unknown: Applicant name in the document contains only one word.

Applicants with “True Positive” and “Potential Match” statuses are delegated to the Compliance Officer for further processing. If applicants are declined based on a watchlist match, they are assigned a respective rejection tag:

- Sanctions
- PEP
- Criminal records
- Adverse Media

In case of positive matches against sanctions lists, the action performed by the MLCO will be in line with the requirements of a specific sanctions program (e.g. asset freeze, rejection, or debt/equity restrictions etc.) as well in consideration with any potential conflict of law.

Sanctions Evasion

UN, U.S., and EU sanctions programs include prohibitions on evasion of their principal provisions, with authorities increasingly focusing on evasion as its own category of sanctioned activity. Examples of attempts to evade sanctions may include:

- Client (natural or legal person) who is not on any applicable sanctions list purchases cryptocurrency on behalf of a business entity owned by a sanctioned party.

- Where a payment is rejected by the Company, and the Client re-issues the payment after changing or removing information, thereby making it difficult to identify and restrict payments to and from sanctioned parties or countries (activity known as “wire stripping”).
- Client physically located in the U.S. utilizes VPN to mask IP address, thereby making it possible to engage in a transaction that is permitted in the EU but prohibited for the US Persons; or
- Payments to a party who is located in a non-sanctioned jurisdiction and acting as a “front company” or acting as an intermediary for sanctioned parties or parties in sanctioned jurisdictions.

Potential sanctions evasion activities may be detected by the Company’s staff at various levels of seniority and across different functions, i.e. through engagement with the existing or prospective Clients, business partners, transaction monitoring, ongoing due diligence (ODD) and other. All suspected attempts to evade or circumvent sanctions must be immediately escalated to the Compliance Officer who, after assessing the scenario, may decide that the case should be escalated to the relevant authorities.

In addition to sanctions screening, the Company utilizes its AML/CTF transaction monitoring, Client due diligence (CDD) and other processes to identify potential sanctions evasion activities by its Clients, third parties, and staff.

When performing the review and approval of Clients identified as high-risk according to the Company’s ML/TF risk assessment methodology, the Compliance Officer also reviews the Client for potential sanctions evasion activities.

The results of the investigation shall be recorded in line with the Company’s AML Policy. Potential sanctions evasion activities, if detected, must be included in the AML/CTF and sanctions compliance reporting documents submitted by the Compliance Officer to the Executive Director(s) and the Board.

Asset Freezing

For the purpose of this Policy, freezing, also known as “blocking”, refers to a form of controlling assets in which a sanctioned party has an interest. While title to blocked property remains with the sanctioned party, the exercise of the powers and privileges normally associated with ownership is prohibited without authorisation from the sanctioning competent authority. Blocking immediately imposes an across-the-board prohibition against transfers or transactions of any kind with regard to the property.

“Assets” refer to tangible or intangible resources with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit. In case of the Geosix B.V. the assets include cryptocurrency and fiat currency.

Sanctions Compliance Training

Sanctions compliance training is one of the pillars of the Company’s sanctions compliance

programme. The Compliance Officer is responsible for reviewing and updating (where required) the sanctions compliance programme.

The compliance training falls under two categories:

1. Annual General Audience (All Staff) training,
2. Risk-Based/Ad-Hoc training to Staff who perform functions considered to be higher risk from a sanctions perspective, such as roles that entail Client contact, processing Client transactions, or otherwise evaluating Client data, must receive additional targeted training to supplement the annual sanctions learning provided to all Staff.

All Staff must receive annual General Audience (All Staff) sanctions compliance training. All new hires must receive the training within 30 (thirty) days of on-boarding. The General Audience (All Staff) sanctions compliance training shall include, at a minimum:

- Major sanctions regimes (UN, EU, UK, US).
- Major sanctions programs and requirements.
- Sanctions evasion methods and techniques.
- Sanctions risk indicators ('red flags').
- Sanctions compliance roles and responsibilities of the Company's staff.
- Consequences of non-compliance.

All training records, including the training content (e.g. presentation slides, post-course assessment) and attendance records must be kept in line with the record-keeping requirements.

Outsourcing

Where a sanctions compliance activity is outsourced to an entity outside the Company, the Company is ultimately accountable for ensuring that such activities are undertaken in compliance with the requirements of this Policy, and all applicable sanctions laws, rules and regulations.

Record-Keeping And Record Retention

The Company adopts one set of record-keeping and record retention rules and requirements to all sanctions-related items as set by the Company's AML Policy.

Appendix IV

Client Acceptance Policy

1. Statement of the Policy

Geosix B.V. is a company duly incorporated under the laws of Curaçao and operates the website <https://vippari.com/en>. The company holds licence number OGL/2024/316/0598, issued by the Curaçao Gaming Control Board, and conducts its activities in full compliance with the licensing conditions and territorial restrictions established by the authorities of Curaçao.

This policy applies to all players from the moment they register an account and begin using the gaming services provided by Geosix B.V. Acceptance of the policy is confirmed either by explicitly agreeing during registration (for example, by selecting a checkbox or responding to a pop-up confirmation) or by continuing to access and use the platform.

Developed in accordance with the requirements and guidance of the Curaçao Gaming Control Board, this policy is an integral part of Geosix B.V.'s wider framework for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). It also aligns with internationally recognised standards, including the recommendations of the Financial Action Task Force (FATF) and the European Union Anti-Money Laundering Directives.

The provisions of this policy complement applicable private law obligations, including those outlined in Book 6 of the Civil Code of Curaçao on general terms and conditions. Nothing within this document limits or diminishes the legal rights of players under relevant civil legislation.

2. Scope of the Policy

This policy applies to all individuals or entities seeking to register an account with Geosix B.V., regardless of the channel through which registration is completed. It includes sign-ups made via the company's official website, mobile applications, affiliate networks, or authorised third-party platforms.

The scope of this policy covers the full customer lifecycle, starting from the initial application for an account and continuing throughout the duration of the relationship until closure or termination. All provisions set out in this document apply to the complete range of products and services offered by Geosix B.V. under its Curaçao gaming licence OGL/2024/316/0598. The Curaçao Gaming Authority (CGA) acts as the supervisory regulator for Geosix B.V. but does not intervene in individual disputes between players and licensed operators. Instead, the CGA uses aggregated complaint data to assess industry-wide compliance and strengthen its regulatory oversight.

Players retain the right to contact the CGA directly if they believe Geosix B.V. has breached licensing obligations, regulatory standards, or engaged in malpractice. The company imposes no restrictions on a player's ability to report such matters to the regulator.

Alignment with Curaçao's Legal Framework

Geosix B.V. considers its Customer Acceptance Policy to be a fundamental part of its wider framework for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF). The policy is designed to comply fully with

Curaçao's legislative framework, including:
National Ordinance on Identification when Rendering Services (NOIS)

National Ordinance on the Reporting of Unusual Transactions (NORUT)

Sanctions National Ordinance (SNO)

Kingdom Sanction Act

National Ordinance on Games of Chance (LOK)

Ongoing Compliance Commitment

Customer acceptance measures are applied throughout the customer lifecycle, not just at onboarding. This ensures that any material changes in a customer's risk profile, behaviour, or jurisdiction are promptly identified and addressed.

Staff Training and Competence

Employees involved in onboarding and verification receive compliance training tailored to Curaçao's legislation and the company's internal standards. This training emphasises:

Effective application of the Risk-Based Approach (RBA)

Identification and escalation of high-risk indicators

Proper use of escalation channels to the Compliance Officer or senior management

Independent Oversight and Audit

Geosix B.V. engages independent auditors at least once a year to review the effectiveness of its Risk-Based Approach and confirm that this policy is applied correctly. The audits cover:

Identity verification procedures

Sanctions and Politically Exposed Person (PEP) screening

Enhanced Due Diligence (EDD)

Ongoing customer monitoring

Audit findings are presented to the Board of Directors, and any deficiencies are addressed promptly through corrective measures with set timelines. This ensures ongoing compliance and the integrity of operations.

3. Customer Acceptance Integration

Geosix B.V. is committed to providing a secure, responsible, and fully compliant gaming environment. Customers are only accepted if they meet all legal, regulatory, and internal compliance requirements.

Age and Identity Verification

Applicants must be at least 18 years of age, or older where required under the laws of their jurisdiction. During registration, players must provide complete and verifiable information, including their full legal name, date and place of birth, nationality, residential address, and a valid government-issued identification document.

Jurisdictional Restrictions

Individuals who reside in, access services from, or transact in prohibited or sanctioned

jurisdictions are not permitted to open an account. These restrictions are applied in line with Curaçao's regulatory framework, international sanctions regimes, and Geosix B.V.'s internal exclusion list. As part of the onboarding process, all applicants are screened against domestic and international sanctions databases, including those maintained by the United Nations, European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Kingdom Sanction Act, the Sanctions National Ordinance, and the Curaçao Gaming Control Board.

Verification of Funds

All funds deposited for gaming must originate from lawful and legitimate sources. If the customer's risk profile indicates higher exposure, Geosix B.V. may request additional documentation to confirm both the source of funds and, where appropriate, the source of wealth.

Right to Refuse Service

Geosix B.V. reserves full discretion to deny services to any individual or entity with a record of fraudulent behaviour, chargebacks, bonus abuse, breaches of gambling regulations, or prior self-exclusion related to gambling harm.

4. Risk-Based Approach

Geosix B.V. applies a thorough Risk-Based Approach (RBA) during both the onboarding process and the ongoing assessment of its customers. This approach ensures that the level of due diligence applied is proportionate to the customer's individual risk profile. The evaluation takes into account a range of factors, including the customer's personal and financial background, the types of products and services they use, any geographic risks associated with their location or funding sources, and potential risks arising from the technologies or channels they use to access the platform.

Customer Risk Profile

Geosix B.V. assesses every prospective customer to determine their level of exposure to risks such as money laundering, terrorist financing, or proliferation financing. This assessment ensures that due diligence measures are applied proportionately to each customer's profile.

Customers who present clear, transparent, and verifiable financial backgrounds for example, those with stable employment in low-risk sectors and gambling activity that aligns with their declared income are typically classified as low risk.

Conversely, customers may be considered high risk if they exhibit certain characteristics, such as having multiple or opaque income sources, employment in industries with elevated AML risk like cryptocurrency or unregulated financial services, or transaction patterns that appear inconsistent with their stated financial profile. Politically Exposed Persons (PEPs), their family members, and close associates are automatically categorised as high risk and are subject to stricter controls.

High-risk cases are managed through Enhanced Due Diligence (EDD), which may include more detailed verification procedures, additional documentation requirements, and ongoing monitoring. Examples of high-risk scenarios include:

- Customers with multiple or irregular income sources, who must provide evidence such as payslips, tax returns, business records, or investment statements.

- PEPs or their close associates, whose accounts require senior management approval, detailed source-of-wealth and source-of-funds checks, and ongoing enhanced monitoring.
- High or disproportionate spenders, where gambling activity exceeds what would reasonably match a customer's financial profile, requiring additional documentation and scrutiny.
- Customers exhibiting sudden, unexplained changes in gambling patterns or those using third parties to transact on their behalf, triggering immediate review and investigation.
- Attempts to operate multiple accounts, which are identified through internal monitoring systems and consolidated for a full transactional review.
- Unknown customers attempting to redeem large volumes of deposits, or customers linked to junket operators, both of which require strict verification and EDD measures.

Geosix B.V. also conducts ongoing monitoring to ensure customer risk profiles remain accurate and up to date. Periodic reviews are scheduled, and additional checks are triggered whenever significant changes are detected, such as unusual transaction patterns, large unexplained deposits, or changes to a customer's personal or financial circumstances. Where risk levels increase, the company applies enhanced controls including EDD, closer transaction monitoring, or restrictions on account activity to ensure risks remain effectively mitigated and regulatory obligations are consistently met.

Geographic Risk Assessment

Geosix B.V. uses a dynamic geographic risk framework to evaluate potential risks linked to a customer's location or the origin of their funds. This framework is regularly updated based on trusted and authoritative sources, including publications and lists from the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the European Commission's high-risk country listings, the U.S. Office of Foreign Assets Control (OFAC), the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from jurisdictions subject to international sanctions are not accepted under any circumstances. Those from high-risk jurisdictions may be considered for onboarding only after Enhanced Due Diligence (EDD) is completed and senior compliance approval is granted.

Jurisdictions are considered high risk when they exhibit one or more of the following characteristics: inadequate anti-money laundering and counter-terrorist financing frameworks or poor enforcement of such measures, systemic corruption that increases the likelihood of illicit funds entering the platform, association with international sanctions related to terrorism or weapons proliferation, or active presence of terrorist organizations.

To maintain accurate classifications, Geosix B.V. continuously monitors relevant global and regional sources. These include FATF high-risk and monitored jurisdictions lists, CFATF advisories, the European Commission's list of countries with strategic AML/CFT deficiencies, OFAC sanctions lists, U.S. State Department reports, and corruption indices or reports indicating potential links to terrorist financing.

When a customer's country of residence or source of funds appears on a high-risk or sanctioned list, the case is escalated to the Compliance Officer. In such instances, EDD measures are mandatory, including in-depth identity verification, a thorough review of the source of funds and source of wealth, and enhanced transaction monitoring for as long as the relationship continues.

Geographic Risk Assessment Process

1. **Initial Screening** – The customer's location and funding sources are checked against global lists and reports to determine their risk level.
2. **Low-Risk Jurisdiction** – The account may be approved under standard due diligence procedures with routine monitoring.
3. **High-Risk Jurisdiction** – The application is escalated to compliance for review. Onboarding is only approved if all EDD criteria are satisfied, and heightened monitoring is applied.
4. **Sanctioned Jurisdiction** – The application is rejected, and records are retained in compliance logs.
5. **Ongoing Monitoring** – Customer profiles are dynamically updated, and additional controls are applied if jurisdictional risk changes over time.

Product, Service, and Transaction Risks

The level of risk associated with a customer is also determined by the products, services, and transaction types they use. Certain activities naturally carry a higher degree of risk due to reduced transparency and traceability. Examples include peer-to-peer transfers, the purchase or exchange of gaming tokens, or the use of anonymous or semi-anonymous payment methods such as prepaid cards or specific cryptocurrencies.

Accounts that are used mainly for financial transactions rather than genuine gameplay such as those making large deposits followed by minimal or no betting activity before withdrawals are treated with caution and subject to closer review. Likewise, the use of payment instruments not registered in the account holder's name automatically triggers additional verification measures to confirm legitimacy.

To mitigate these risks, Geosix B.V. actively monitors and manages several key risk areas. Funds deposited into gaming accounts must always originate from lawful and verifiable sources. If there are signs that funds may be linked to criminal activities such as fraud, theft, or trafficking, customers are required to provide evidence of the legitimate source of those funds, and any suspicious transaction is reported to the Financial Intelligence Unit (FIU) in line with legal requirements.

Anonymous or semi-anonymous payment channels, including prepaid cards and certain virtual assets, are treated as high risk and subject to enhanced verification procedures, with full documentation of the source of funds. Accounts must also be used solely for genuine gaming purposes. Any behaviour suggesting misuse, such as depositing and withdrawing without significant gameplay, triggers an immediate review and may lead to account suspension during investigation.

Transactions involving third-party payment methods are flagged and subject to full

verification of both the customer and the third party, including establishing the relationship between them and confirming the legitimacy of the funds. Similarly, transfers between gaming accounts are generally prohibited unless a legitimate and documented reason exists, in which case approval from the Compliance Officer is required, and full records of the transaction are maintained.

Operating multiple accounts or wallets including those on different platforms under the company's control is considered a red flag. Internal monitoring systems are designed to detect and link related accounts, ensuring consolidated oversight and the ability to conduct a thorough review of all connected activity. Customers who frequently change their payment methods or banking details may also be attempting to obscure the origin of funds; such patterns prompt a detailed profile review and, where appropriate, the application of Enhanced Due Diligence (EDD).

Geosix B.V. applies robust identity verification and authenticity checks to prevent and detect identity fraud. Any suspected cases are escalated to the relevant authorities in line with regulatory obligations. Additional controls are applied to the use of electronic wallets, particularly where providers are licensed in jurisdictions with weak AML or CTF oversight or where their structures make it difficult to trace funds. Customers using e-wallets are required to verify the source of their funds, and the provider's licensing and compliance standards are checked before any transaction is approved.

Channel and Technology Risk

The level of risk associated with a customer also depends on the channels and technologies used to access Geosix B.V.'s services. Remote onboarding, while convenient, carries a higher risk of identity fraud or impersonation. To address this, the company relies on advanced digital Know Your Customer (KYC) solutions that include biometric verification, document authenticity checks, geolocation validation, and multi-factor authentication.

Before introducing any new technologies, payment solutions, or platform features, Geosix B.V. conducts a comprehensive risk assessment to ensure the innovation cannot be misused for money laundering, fraud, or other illicit purposes.

Several factors are monitored closely to manage channel and technology-related risks. Any method that allows customers to remain anonymous is considered high risk and triggers enhanced verification measures. These measures include identity document validation, biometric checks, and real-time screening against sanctions and Politically Exposed Person (PEP) lists.

Remote interactions, although common in the industry and not inherently high risk, still demand strong safeguards. Geosix B.V. uses secure verification technologies such as biometric checks, liveness detection, and automated document validation to prevent impersonation and fraud during onboarding and transactions.

When third parties are involved in customer interactions, the risk profile increases, especially if the intermediary is not subject to AML/CFT obligations. In such cases, Geosix B.V. performs due diligence not only on the customer but also on the third party. This process includes verifying the intermediary's regulatory status, assessing its compliance framework, and ensuring all provided information is accurate and verifiable.

Risk Indicators

Geosix B.V. applies a structured set of risk indicators to assess the level of risk associated with every customer relationship. These indicators form part of the company's Risk-Based Approach (RBA) and ensure that the level of due diligence applied is always proportionate to the customer's overall risk profile.

The evaluation covers multiple categories:

- **Customer Risk Profile** – factors such as multiple or irregular income sources, Politically Exposed Persons (PEPs), high or disproportionate spending, sudden changes in spending behaviour, involvement of third parties, multiple accounts, unknown chip redemptions, or links to junket operations.
- **Product, Service, and Transaction Risk** – warning signs such as proceeds of crime, anonymous or unregulated payment methods, misuse of accounts, third-party funding, frequent changes in payment instruments, identity fraud, or the use of multiple e-wallets.
- **Geographic Risk** – customers connected to jurisdictions with weak AML/CFT frameworks, high levels of corruption, international sanctions, terrorism links, or countries listed by FATF, CFATF, OFAC, or Transparency International's CPI.
- **Channel and Technology Risk** – customers accessing services through anonymous or unverified channels, onboarding remotely without sufficient identity validation, or relying on unregulated third-party intermediaries.

To determine the customer's overall risk, the company uses an internal Risk Calculator that assigns a weighted score to each indicator. The total score determines the customer's classification:

Risk Level	Requirements
Low Risk	Standard Customer Due Diligence (CDD) applies, with documentation limited to what is legally required or triggered by a change in risk profile.
Medium Risk	Standard CDD plus additional verification steps and closer ongoing monitoring.
High Risk	Full Enhanced Due Diligence (EDD), senior management approval prior to onboarding, and enhanced ongoing monitoring.

This risk-scoring approach ensures a consistent and methodical assessment of customers, allowing the company to allocate its resources effectively and meet its regulatory obligations.

Risk Indicators Table

Factor	Low Risk	Medium Risk	High Risk
Purpose of Account	Recreational or casual gaming.	Professional-level gambling or consistent high-stakes play.	Bonus exploitation or behaviour aimed at financial abuse of promotions.
Source of Funds	Regular salary, savings, pensions, or other low-risk income.	Business income, legitimate casino winnings, sale of personal assets, inheritance, or documented loans/gifts from family or friends.	Unverified cryptocurrency, offshore accounts, or other unverifiable sources.
Source of Wealth	Long-term employment income, ownership of established businesses, verified inheritance, or steady investment growth.	Sale of property or business, significant lottery or gambling winnings.	High-risk investments such as cryptocurrency or forex trading, offshore holdings, or unverifiable assets.
Transaction Frequency	Occasional, typically monthly.	Regular, often weekly.	Frequent, typically daily.
Transaction Value (NAF)	Up to 1,000.	Between 1,000 and 4,000.	Over 4,000.
Incoming Payments	Standard bank transfers or debit/credit card deposits.	E-wallet or prepaid card deposits.	Cryptocurrency, third-party funding, deposits from high-risk jurisdictions, unusually high deposits, or use of unregulated processors.

Outgoing Payments	Normal withdrawals of winnings or deposit refunds.	Bonus-related frequent withdrawals, or large single withdrawals above 4,000.	Cryptocurrency withdrawals, third-party payments, chargebacks, or suspicious withdrawal patterns linked to other accounts.
Gaming Behaviour	Casual, moderate, and consistent play patterns.	Frequent high-stakes betting, extended play sessions, or fluctuating wagering amounts.	Aggressive betting patterns, rapid stake increases, loss-chasing, multiple accounts, collusion, or other fraudulent indicators.
Payment Channels	Traditional bank transfers.	Verified e-wallets.	Cryptocurrency or other anonymous or unverified payment methods.
Adverse Media	No negative information identified.	Questionable or unverified reports of misconduct.	Confirmed involvement in criminal or illicit activities.

Guidance on Using the Risk Indicators

These indicators are designed to help staff assign an accurate risk profile to each customer during onboarding and throughout the customer relationship. Each factor should be assessed individually, and the combined results should inform the overall risk classification.

- Customers with mostly low-risk indicators are assigned a low-risk profile and subject to standard Customer Due Diligence (CDD).
- Customers with a mix of low and medium-risk indicators are classified as medium risk and require additional verification and closer monitoring.
- Customers displaying one or more high-risk indicators must undergo Enhanced Due Diligence (EDD), senior management approval before onboarding, and ongoing heightened monitoring.

Risk profiles should be reviewed regularly and adjusted when customer behaviour, transaction patterns, or external risk factors change. This approach ensures that the company's risk management remains dynamic and aligned with regulatory expectations.

5. Onboarding Procedures

Geosix B.V. follows a structured and well-documented onboarding process to ensure that only customers meeting the company's acceptance standards gain access to the platform. No account is activated until the customer has successfully completed all required identification, verification, and sanctions screening steps.

During registration, customers are required to provide their full legal name, date and place

of birth, nationality, residential address, and an official identification number such as a passport or national ID.

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

If a customer is identified as high risk during the initial assessment, additional verification is required. This includes providing documentation to confirm the legitimacy of their funds and, where relevant, the source of their wealth. Acceptable documents may include recent bank statements showing income deposits, business account records or financial statements, tax returns, contracts of property or asset sales, and investment account statements. These enhanced measures ensure that the company meets regulatory expectations and maintains a strong control framework to protect the platform from misuse.

Client Identification requirements and verification procedures

This section refers to individuals who directly or indirectly establish a business relationship with the Company (e.g. direct Clients, beneficial owners, authorized persons, etc.). The Company should be satisfied that it is dealing with a real person and obtain sufficient evidence of identity to establish that a prospective Client is who he/she claims to be.

Document verification is intended to prevent the following issues:

Forgery
Data tampering
Photo replacement
Fraud
Using document printouts
Other manipulation

The ID document must contain as minimum the following information:

Owner full name
Owner full date of birth
Document number
Validity data (issue date or validity period)
Owner photo
Owner signature (if applicable)

The ID document should meet the following requirements:

- The document is valid for at least one month from the upload date.
- The document is not scratched, stained, or torn.
- The applicant full name, date of birth and other important information is present and can be read.

Uploading the photo of an ID document

The photo of the ID document uploaded to the system should meet the following requirements:

The uploaded file is an original photo (static image) or scan (not a screenshot or a photo uploaded from social networks) in JPG, JPEG, PNG, PDF.

If the document has data on the front and back, both sides should be uploaded.

The size of the uploaded file is no less than 100 KB or 300 DPI.

The photo is in color.

The information in the document is readable.

All corners of the document are visible and no foreign objects or graphic elements are present.

The uploaded photo has not been edited with any software or converted to PDF.

The document is not digital (in most cases).

Checking the image for authenticity

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Document data validation

At the final step, the data extracted from the document is checked against various sources, including sanctions and watchlist databases.

1. Proof of address verification

a. Face-to-face procedures

For the purpose of face-face Client identification, the MLCO shall inspect the person's original Proof of Address (PoA) documentation and make a certified true copy to be maintained as evidence of verification.

b. Non-face to face procedures

The process of Proof of Address (PoA) document verification for non-face to face Clients consists of the following steps:

- **Uploading a PoA photo.**

By default, the system accepts PoA documents that have been issued within the last 3 months.

- **Checking the image for authenticity.**

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software

signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image receives a digital trust score:

- Low – red (high risk of editing).
- Acceptable – yellow (there might be something to take a closer look at).
- Normal – green (a trusted and authentic image).

- **Checking the integrity of the image.**

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents. Integrity checks consist of:

- General conformity to the template.
 - Font originality and compliance with the relevant standards (width, spaces between the letters, and so on).
 - Required fields and inscriptions.
-
- **Data extraction** (full name, home address, issue date).
 - **Data validation** (whether the address is complete, if it exists and if it is really a home address).

To ensure the completeness and consistency of the extracted address data, external map services, such as Google Maps, Open Street Map, and others, are utilized allowing the MLCO to see the applicant's geolocation in the Dashboard.

Supported PoA Documents

Common proof of residency examples:

- Tax bill (not older than 3 months).
- Mortgage statement.
- Certificate of voter registration.
- Correspondence with a government authority regarding the receipt of benefits such as a pension, unemployment benefits, housing benefits, and so on.
- Cable internet/TV bill (but not from satellite TV companies or for other wireless telecommunication services).
- Landline telephone bill.
- Bank statement with the date of issue and the name of the person (the document must be not older than 3 months).
- Utility bill for gas, electricity, water, internet, etc. linked to the property (the document must not be older than 3 months).

- A lease agreement that is current and has the signatures of the landlord and the tenant.
- Rent bills issued by a real estate rental agency.
- Credit card statement issued by a bank.
- Letter from a recognized public authority or public servant (any government-issued correspondence not older than 3 months).
- Employer's certificate for PoA.
- House purchase deed.
- The document must contain the full name, home address, and the document issue date (in most cases). Both paper documents and electronic documents (in PDF) are accepted.

Alternative proof of residency examples

The following documents can also be accepted as valid PoA, but only if they contain an address:

- Passport
- Identity card
- Driving license
- Residence permit (EU samples containing address)

**** The same document cannot be used to confirm both an identity and a place of residence. So, if an applicant submits an ID document as PoA, they should use another document to confirm their identity.*

Documents which are not acceptable as Proof of Address, include:

- Old government-issued correspondence (older than 3 months)
- Old bank statements (older than 3 months)
- Old utility bills linked to the property (older than 3 months)
- Pension statements
- Bank references
- Insurance policies
- Mobile phone bills
- Medical bills
- Receipts for purchases
- Insurance statements
- Documents stating PO Box addresses
- Checks
- Envelopes and parcels showing your name and an address
- Prepaid card invoices
- Mobile sim cards+ bills issued to a business address
- Bills from debt collection agencies

- Bills from fintech companies
- Papers referring to discount cards which cannot be considered as bank cards
- Car rent bills

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

SoF refers to origin of funds being deposited, received, or transferred with the Company. SoF tells us where the money is coming from, which can be proven through bank statements, tax returns or the Company financials, etc.

Typically, SoW is requested when establishing business relationships or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

Examples of SoW and SoF and supporting documentation that can be provided, include:

1. Income from Salary

To verify income derived from employment, the following documents are required:

- Pay slips for the previous three (3) months and a bank statement showing the salary being deposited into the customer's account;
- An audited personal tax statement.

2. Inheritance

To evidence funds originating from an inheritance, the customer must provide:

- A Grant of Probate (with a copy of the Will) clearly indicating the amount inherited, along with a bank statement showing the inheritance funds entering the account;
- Alternatively, a signed letter from a licensed solicitor or estate trustee on official letterhead confirming the amount inherited, accompanied by proof of the solicitor's regulated status and a bank statement showing deposit of the inheritance funds.

3. Gift or Donation

For funds originating from a gift or donation, the following must be provided:

- A notarized gift/donation letter and a bank statement showing deposit of the gifted funds;
- Or a formal gift agreement together with a bank statement showing the funds being deposited.

4. Savings or Deposits

Funds derived from accumulated savings or deposits must be supported by:

- A savings account statement;
- A bank statement demonstrating the availability of funds.

5. Government Grants (e.g., retirement income, veterans' benefits, research grants)

Customers must provide:

- Documentation identifying the type of grant received and a bank statement showing grant funds entering the account;
- Additional documents confirming the grant entitlement, accompanied by a bank statement showing the deposits.

6. Company Profit / Dividends

Where the customer's funds originate from business profits or dividends, the following are required:

- Dividend contract note or equivalent documentation, along with a bank statement showing receipt of dividend funds;
- A copy of the most recent audited financial statements;
- A tax declaration form.

7. Loans or Investments

For funds sourced through loans or investment proceeds, the customer must provide:

- A loan or investment agreement, or other supporting documentation confirming the arrangement, and a bank statement showing the funds being deposited.

8. Sales (Property, Goods, Shares, etc.)

To verify funds resulting from sale transactions, the customer must provide:

- A copy of the sale, purchase, or production contract and a bank statement showing the deposited proceeds;
- Proof of online sales (such as an e-commerce sales report or screenshot listing sold items), together with a bank statement showing the deposits;
- Shipping or delivery documents, where applicable;
- Customs declarations (for cross-border goods);
- Audited financial reports or tax reports, if relevant;
- Any statement or formal document evidencing receipt of sale proceeds and the corresponding bank statement showing the deposit.

6. Ongoing Monitoring

Geosix B.V. recognises that customer acceptance is an ongoing process rather than a one-time activity. Continuous monitoring is essential to ensure that customer behaviour remains consistent with the profile established during onboarding and that any irregularities or deviations are promptly identified and addressed.

The company uses automated transaction monitoring systems to detect patterns of unusual or suspicious behaviour. Alerts are generated for activities such as deposits or withdrawals that do not match the customer's declared profile, rapid movement of funds without meaningful gameplay, the use of multiple or unusual payment methods, or patterns that may suggest collusion, chip-dumping, or other prohibited activities.

Each alert is reviewed by trained compliance officers, who assess the circumstances and determine whether further investigation or escalation is needed.

In addition to real-time monitoring, the company conducts periodic reviews of customer profiles on a risk-based schedule to ensure risk ratings remain accurate. If there are material changes in a customer's situation, such as relocation to a high-risk jurisdiction, significant increases in transaction values, or changes in funding methods, the customer's risk profile is immediately reassessed. Where necessary, enhanced monitoring and other controls are applied to maintain compliance and mitigate potential risks.

7. Prohibited clients and transactions

Certain types of Client/transactions are not accepted for establishing business relationships or conducting transactions in order to reduce the risk that the services and products of the Company may be used for money laundering or terrorist financing or other illicit purposes and at the same time for protect the Company from the financial, reputational and legal risks.

Consequently, it is strictly prohibited to:

- c. Establish a business relationship with Clients who fail or refuse to submit the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification.
- d. Establish a business relationship and/or conduct transactions with natural or legal persons against which sanctions prohibiting such relationship/transactions are imposed in accordance to the Company's Sanctions Policy (Appendix II).
- e. Conclude or implement any business relationship with a credit institution or other financial institution or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions or legal person that is incorporated in a jurisdiction in which it has no physical presence, involving meaningful management and which is unaffiliated with a regulated financial group (i.e. shell company) or is known to permit accounts to be held by a shell bank.
- f. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons whose activities are related to criminal activity including (but not exhaustive)
 - Terrorist offences, offences related to a terrorist group and offences related to terrorist activities as set out on Titles II and III of Directive (EU) 2017/541 (replacing Framework Decision 2002/475/JHA on combating terrorism)
 - Any of the offences referred in article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
 - The activities of criminal organizations as defined in Article 1(1) of Council Framework Decision 2008/841/JHA on the fight against organized crime;
 - Trafficking in human beings and migrant smuggling, including any offence set out in Directive 2011/36/EU;
 - Sexual exploitation, including any offence set out in Directive 2011/93/EU;
 - Fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1 (1) and Article 291) of the Convention on the protection of the European Community's financial interests;
 - Corruption, including any offence set out in the Convention on the fight against corruption involving officials of the EU Communities or officials of Member States of the EU;
 - All offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the international laws and which are punishable by deprivation of liberty or a detention order;
 - Counterfeiting of currency, including any offence set out in Directive 2008/99/EC;
 - Cybercrime, including any offence set out in the Directive 2013/40/EU;
- g. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons where:

- Legal entities are owned through bearer instruments;
 - Legal entities are involved in the adult industry;
 - Legal entities are involved drugs industry;
 - Legal entities are involved in arms industry;
 - Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients acting on behalf of Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients whose source of funds (SoF) and source of Wealth (SoW) were generated from a sanctioned activity;
 - Clients whose source of funds (SoF) and source of Wealth (SoW) cannot be verified when this is required;
 - Purchase or sale of virtual assets ultimately owned or controlled, directly or indirectly, by sanctioned parties;
 - Transactions with third parties ultimately owned or controlled, directly or indirectly, by sanctioned parties;
- h. Establish a business relationship and/or conduct transactions with natural or legal persons residing in a jurisdiction/country where it is prohibited by Company policy to offer its services to. Prohibited jurisdictions / countries shall include:

Unrecognised / Disputed Territories

Crimea	Republic of Abkhazia
Donetsk	Republic of China (Taiwan)
Luhansk	Republic of Kosovo
Nagorno Karabakh Republic	Republic of Somaliland
Palestine	Republic of South Osetia
	Turkish Republic of Northern
Pridnestrovian Moldavian Republic	Cyprus

Prohibited Jurisdictions / Countries

Australia	Libya
Belarus	Mali
Belize	Netherlands
Central African Republic	North Korea
Cuba	Russia
Curaçao	Somalia
Democratic Republic of Congo	Sudan
Dutch West Indies (Aruba, Bonaire)	Syria
France	Turkish Republic of Northern
	Cyprus
Germany	UK
Iran	USA
Iraq	Yemen
Lebanon	Libya

8. Enhanced Due Diligence (EDD)

The Company acknowledges that its obligations regarding customer identification, verification, and ongoing due diligence arise from the January 2025 AML/CFT/CPF Regulations, specifically Part III, Articles 14–27, which mandate risk-based CDD, enhanced due diligence for high-risk clients, identification of beneficial owners, source-of-funds verification, and continuous monitoring of business relationships.

Enhanced Due Diligence (EDD) procedures are applied to customers who present an elevated risk profile. This includes Politically Exposed Persons (PEPs), their family members, and close associates; customers based in or funding their accounts from high-risk jurisdictions; those conducting unusually large, complex, or unexplained transactions; and customers whose financial behaviour is inconsistent with their declared income or business activities.

EDD involves a more detailed and rigorous verification process than standard due diligence. This includes a full analysis of the customer's source of funds and source of wealth, supported by credible and independent documentation. Additional steps include corporate registry and public record searches to verify legal and beneficial ownership, confirmation of employment or business ownership, reviews of audited financial statements or other reliable financial documents, and thorough adverse media and reputational checks.

Senior management approval is required before onboarding any high-risk customer, and in complex or sensitive cases, formal approval from the Board of Directors may be necessary.

Once these customers are onboarded, they are subject to ongoing enhanced monitoring. This includes lower thresholds for triggering transaction reviews, closer scrutiny of their transaction patterns, and more frequent reassessments of their risk profiles. These measures ensure that higher-risk relationships are managed appropriately, in full alignment with both regulatory obligations and the company's internal risk appetite.

Prohibited Customer Categories

Geosix B.V. will not onboard or will immediately terminate relationships with customers who meet any of the following criteria:

- Anonymous or unverifiable customers, including those who fail or refuse identity verification within 30 days.
- Shell companies, fictitious entities, or customers with unclear beneficial ownership.
- Sanctioned individuals or entities, including those appearing on UN, EU, OFAC, OFSI, SNO, or Kingdom Sanction Act lists.
- Residents of or transacting from prohibited or sanctioned jurisdictions, as defined in Section 4 (Geographic Risk).
- Customers below the legal age for gambling.
- Customers involved in fraud, bonus abuse, identity theft, or other illicit behaviour.
- Third-party transactors or users of anonymous payment channels without valid justification or verification.
- Customers whose source of funds or source of wealth cannot be verified or is linked to crime.

Acceptance and Rejection Triggers

Customer applications will be immediately rejected or suspended when any of the following triggers occur:

a. Documentation and Verification Failures

- Refusal to provide KYC, proof of address, or EDD documentation.
- Submission of false, altered, or misleading information.
- Failure to complete mandatory verification within 30 days.

b. AML/CTF/CPF Risk Triggers

- Positive sanctions match or verified PEP hit without manageable risk.
- Suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.
- Inability to verify SOF/SOW after reasonable attempts.

c. Behavioural and Transactional Triggers

- Highly unusual deposit/withdrawal activity inconsistent with profile.
- Multiple accounts, third-party payments, or misuse of payment instruments.
- Attempts to circumvent controls or operate through intermediaries.
- Evidence of collusion, chip dumping, or non-genuine gameplay.

9. Termination

Geosix B.V. reserves the right to suspend or terminate any customer relationship when required by regulations, internal policies, or risk considerations. This action may be taken if a customer fails to provide the requested identification or supporting documentation within 30 calendar days, if there is reasonable suspicion of money laundering, terrorist financing, or proliferation financing, or if the customer engages in activities that violate applicable laws, regulations, or the company's Responsible Gambling Policy.

When a relationship is terminated due to suspected criminal activity, the company promptly files a report with the Financial Intelligence Unit (FIU) in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds in the account are returned to the original funding source unless there is a legal requirement to freeze or seize the funds pending investigation. Detailed records of all termination actions, including the rationale and supporting evidence, are maintained for at least five years.

Geosix B.V. will refuse to onboard or will terminate an existing relationship in cases where:

- The customer is a resident of, located in, or conducting transactions from a prohibited or sanctioned jurisdiction.
- The customer fails to provide required information or documentation within the specified timeframe.

- False, misleading, or incomplete information is provided during registration or verification.
 - The source of funds or source of wealth cannot be confirmed as legitimate.
 - The customer is involved in, or suspected of, money laundering, terrorist financing, or other criminal activity.
 - The customer is a Politically Exposed Person (PEP) whose risk profile cannot be mitigated to an acceptable level.
- Fraudulent activities, bonus abuse, collusion, or prohibited gambling behaviour are detected.
- The customer attempts to use third parties to transact without proper disclosure and verification.
 - The customer has self-excluded or been excluded for responsible gambling reasons.
 - Large chip redemptions or withdrawals are requested without verifiable linked gambling activity.
 - The customer is a minor or below the legal gambling age in their jurisdiction.

10. Curaçao's Legislative Framework

Geosix B.V. acknowledges that its Customer Acceptance Policy is an integral part of its wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The policy is designed to fully comply with Curaçao's legal and regulatory requirements, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Compliance with these obligations is treated as a priority in daily operations. The customer acceptance procedures are embedded within the company's compliance processes to ensure due diligence is continuous and extends beyond onboarding. This approach ensures that any significant changes in a customer's risk profile, transactional behaviour, or jurisdiction are identified and addressed promptly.

All employees involved in onboarding and verification activities receive dedicated training to help them understand the legislative framework and the company's internal standards. The training focuses on effectively applying the Risk-Based Approach, identifying and escalating high-risk indicators, and following escalation protocols to the Compliance Officer or senior management.

Independent audits are conducted at least annually to evaluate how effectively the Risk-Based Approach and the Customer Acceptance Policy are being implemented. These audits review critical processes, such as identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD) procedures, and the ongoing monitoring of customer activities. The findings are reported to the Board of Directors, and any gaps or deficiencies are addressed promptly through corrective measures implemented within defined timeframes.

11. Responsible for Gambling Integration

Geosix B.V. ensures that its Customer Acceptance Policy is fully aligned with its

Responsible Gambling Policy, recognising that protecting customers from gambling-related harm is a key part of its compliance and operational framework.

If a customer shows behaviour that indicates potential harm, such as frequent deposits that exceed their apparent financial capacity or excessively long gaming sessions, the company takes immediate action. Depending on the situation, this may include setting deposit or wagering limits, temporarily suspending the account, or, in severe cases, refusing further access to services to protect the customer.

Self-exclusion requests are handled promptly and applied to all accounts linked to the customer to ensure these measures cannot be bypassed. These restrictions remain active for the period specified by the customer or as required by regulatory standards.

Employees in customer-facing roles receive targeted training to help them identify early signs of problem gambling. This training is incorporated into both the onboarding process and ongoing monitoring activities, enabling timely intervention when risk indicators are observed.

12. Review and Governance of CAP

This Customer Acceptance Policy is reviewed by Geosix B.V. at least once every twelve months to ensure that it remains effective, relevant, and aligned with applicable legislation, regulatory expectations, and recognised industry standards.

The review process takes into account:

Adjustments to the company's overall risk exposure

Emerging trends in customer behaviour

Technological developments that may introduce new risks

Any proposed amendments are prepared by the Compliance Officer and submitted to the Board of Directors for formal approval prior to implementation. All revisions are fully documented, and relevant employees are promptly informed and trained to guarantee that the updated policy is consistently applied throughout the organisation.

13. Record Keeping

Geosix B.V. maintains comprehensive records connected to customer acceptance for a minimum of five years following the termination of a business relationship, in line with Curacao's regulatory requirements. These records include:

- Identification and verification documents
- Proof of residence
- Evidence of the source of funds and, where required, the source of wealth
- Alerts generated by transaction monitoring systems
- Investigation reports and compliance reviews
- Files relating to Enhanced Due Diligence (EDD)
- Documentation of account suspensions or terminations

All records are stored securely in encrypted systems and protected through strict access controls to ensure confidentiality and data integrity. Access is restricted to authorised staff only, with every instance of access logged and subject to periodic review to verify compliance with internal procedures and data protection obligations.

