

Investan N.V.

AML Policy

Version: 2.0

Last Update: 2025-11-01

Applicability: Investan N.V.

License: CGA License Number OGL/2024/1630/1008

Owner: Compliance (RG) Officer

Approver: CEO

Security Class: Internal

Revision History

Ver.	Date	Author	Comment
2.0	2025-11-01	Compliance Officer	Policy updated for CGA compliance
2.0	2025-12-01	CEO	Approval

AML Policy (CGA)

Investan N.V.

Table of Contents

1. INTRODUCTION AND POLICY STATEMENT	4
1.1 Policy Statement and Commitment	4
1.2 Scope and Application	5
1.3 Regulatory Framework	5
2. RISK-BASED APPROACH FRAMEWORK	7
2.1 Risk-Based Approach Principles	7
2.2 Business Risk Assessment (BRA)	7
2.3 Customer Risk Assessment (CRA)	8
2.4 Risk Factor Categories	9
2.5 Risk Assessment Documentation and Review	9
2.6 National Risk Assessment Integration	10
2.7 New Product/Technology Risk Assessment	11
3. GOVERNANCE AND ORGANIZATION	13
3.1 AML Program Components	13
3.2 Senior Management and Board Responsibilities	13
3.3 Compliance Officer Appointment and Role	14
3.4 Compliance Officer Responsibilities	15
3.5 Internal Controls Framework	16
3.6 Process for Regulatory Updates	17
4. CUSTOMER DUE DILIGENCE FRAMEWORK	18
4.1 CDD Principles and Prohibitions	18
4.2 CDD Triggering Events and Thresholds	18
4.3 CDD Measures Overview	19
4.4 Customer Identification Requirements	19
4.5 Customer Verification Requirements	19
4.6 Beneficial Owner Requirements	21
4.7 Business Relationship Purpose and Customer Profiling	21
4.8 CDD Timing and Account Management	21
4.9 Enhanced Due Diligence (EDD)	22
4.10 Simplified Due Diligence (SDD)	23
4.11 Politically Exposed Persons (PEPs)	24
4.12 Ongoing Monitoring	26
4.13 Existing Customer Application	26
4.14 Business Relationship Termination	27
4.15 Third Party Reliance	27
4.16 Tipping-Off Considerations	28
4.17 Sanctions Framework	29

AML Policy (CGA)

Investan N.V.

5. TRANSACTION MONITORING AND REPORTING	30
5.1 Unusual Transaction Recognition Framework	30
5.2 Unusual Transaction Categories	30
5.3 Staff Training and Internal Reporting	31
5.4 Complex and Large Transaction Monitoring	31
5.5 External Reporting Procedures	31
5.6 Internal Decision Documentation	32
5.7 Disclosure Prohibitions and Tipping-Off	32
6. TRAINING AND AWARENESS	33
6.1 Training Program Framework	33
6.2 Employee Screening	33
6.3 Role-Specific Training Requirements	33
6.4 New Employee Training	34
6.5 Front-Line Staff Training	34
6.6 Specialized Training	34
6.7 Management Training	35
6.8 Refresher Training	35
6.9 Training Documentation	36
7. AUDIT AND INDEPENDENT REVIEW	37
7.1 Independent Audit Requirements	37
7.2 Audit Scope and Testing	37
7.3 Audit Documentation and Reporting	38
7.4 Program Testing and Adaptation	38
8. RECORDS AND DOCUMENTATION	39
8.1 Record Retention Requirements	39
8.2 Regulatory Access Requirements	39
8.3 CGA Examination Documentation	40
8.4 Documentation Standards	40
9. POLICY MAINTENANCE AND REVIEW	41
9.1 Policy Review and Updates	41
9.2 Policy Approval and Communication	41
9.3 Non-Compliance and Escalation	42

1. INTRODUCTION AND POLICY STATEMENT

1.1 Policy Statement and Commitment

As a gaming operator licensed under the jurisdiction of Curaçao, the Company is fully committed to preventing the abuse of our platform, products, and services for the purposes of money laundering, terrorist financing, or the financing of proliferation. The company operates with full awareness of the risks inherent to the online gambling sector and maintains the highest standards of regulatory compliance, integrity, and corporate responsibility.

Money laundering (ML) is defined as the process of concealing the origins of illicitly obtained funds so that they appear to come from a legitimate source. This typically involves a series of financial transactions designed to obscure the source, movement, and ownership of the funds. Terrorist financing (TF), by contrast, involves the provision or collection of funds intended to be used—directly or indirectly—for terrorist acts, regardless of whether the funds originate from legal or illegal sources.

Despite these differences, both ML and TF involve financial transactions and value movements, such as between individuals, accounts, institutions, countries, or asset classes. Both are focused on concealing the origins and destinations of the funds.

The company has implemented internal security measures to prevent money laundering and terrorist financing. These measures are designed to monitor high-risk customers and identify suspicious behaviors, including those related to predicate offenses of money laundering and terrorist financing. The company is further approved to accept and transact with customers in crypto (digital or virtual) currencies.

The company adheres to strict codes of conduct in order to protect the company's good standing, instill trust with the customers, comply with regulatory requirements, and fulfil its ethical responsibility.

The company adopts a zero-tolerance approach to all forms of financial crime and has implemented a comprehensive framework of internal controls, including risk-based customer due diligence, transaction monitoring, and escalation procedures for suspicious activity. These controls are continuously reviewed and aligned with evolving international standards, including those of the FATF.

To ensure full operational effectiveness, all staff are subject to mandatory AML/CFT training and are equipped to identify red flags, understand their reporting obligations, and act in accordance with both local and international regulations, high ethical standards, and internal compliance practice.

The company is dedicated to preserving the integrity of the financial system, protecting our customers and stakeholders, and contributing meaningfully to the

AML Policy (CGA)

Investan N.V.

global effort to combat money laundering and the financing of terrorism.

1.2 Scope and Application

Company, Investan N.V., incorporated under the laws of Curaçao with company number 153108 and a registered office at Zuikertuintjeweg Z/N Zuikertuin Tower Curacao (hereinafter referred to as “the Company”), has appointed a Compliance Officer in accordance with best AML practices.

This policy is applicable to all employees and outsourced staff involved in anti-money laundering, responsible for remote gaming activity, and anti-fraud procedures as they relate to their respective duties, including senior management and the Compliance Officer.

The Compliance Officer, who is primarily responsible for preventing money laundering and the financing of terrorism, is also responsible for ensuring ongoing regulatory compliance and overseeing anti-money laundering procedures.

The Compliance Officer will be actively involved in developing and managing the processes required to combat money laundering and other fraudulent activities based on the following key principles:

- The Company operates on the assumption that the majority of its customers are not engaged in money laundering. However, in compliance with applicable regulations, it uses a risk-based approach to verify player identities;
- The Company monitors all transactions and activities;
- The Company conducts continuous monitoring of its customers, associated risks, and internal processes.

The Company will ensure that all relevant employees receive training on AML and CTF policies and procedures, emphasizing awareness of these risks. All applicable employees must pass competency assessments on these topics.

1.3 Regulatory Framework

The Company’s Policy and Procedures have been developed in accordance with the relevant applicable legislation, including but not limited to the following:

- Curaçao - National Ordinance Reporting Unusual Transactions (NORUT) of November 7, 2017;
- National Ordinance Identification when Rendering Services (NOIS) of October 2, 2017;
- National Ordinance Penalization of Money Laundering (NOPML)

AML Policy (CGA)

Investan N.V.

- EU-Directive 2015/849 of the European Parliament and of the Council of 20 May 2015;
- EU-Directive 2018/843 of the European Parliament and of the Council of 30 May 2018;
- EU-Directive 2018/1673 Of the European Parliament and Of the Council Of 23 October 2018;
- The FATF Recommendations.

The Company tracks amendments of Sanctions Decrees and Regulations on a regular basis and updates and AML policy and procedures accordingly.

2. RISK-BASED APPROACH FRAMEWORK

2.1 Risk-Based Approach Principles

The Company is committed to preventing and combating money laundering and terrorist financing by employing a Risk-Based Approach (RBA).

This approach is implemented on the following levels:

- Risk identification and assessment – Identifying the money laundering risks the Company faces, considering its customer base, products, and services, as well as relevant available information, and evaluating the potential scale and impact of these risks;
- Risk mitigation – Implementing appropriate measures to reduce the significant risks that the Company may encounter;
- Risk monitoring – Establishing management information systems (MIS) to continuously track changes in the risk profile, whether from business developments or evolving threats;
- Documentation – Recording the risk assessment and strategy, ensuring policies and procedures cover these areas, and securing effective accountability from the board and senior management.

The RBA is mainly documented in the following policy documents:

1. Business Risk Assessment (BRA).
2. Customer Acceptance Policy (CAP) and Customer Risk Assessment (CRA).

2.2 Business Risk Assessment (BRA)

The Business Risk Assessment identifies and evaluates risks, including distribution channels risks, associated with the Company's overall operations, taking into account:

- The nature and complexity of products and services offered;
- Customer base and target markets;
- Delivery channels (e.g., face-to-face, online, intermediaries);
- Geographic exposure, including countries of operation and counterparties;
- Industry sectors involved.

The business risk assessment considers all factors that may have an impact on the risks of money laundering, financing of terrorism, and financing of proliferation must be taken into account in the risk assessment, but special consideration must be given to the type of customers, products and services offered, delivery channels, and geographical risk factors. Once the business risk has been assessed, the Company sets

a risk appetite to decide how much risk it is prepared to accept.

The effectiveness of the implementation of these measures must be monitored and improved where necessary.

The Company has to revise its business risk assessment whenever there are changes to the environment within which the Company operates and within business activities, such as the introduction of new payment methods, new markets, new games, or regulatory changes. In the absence of changes, the Company assesses its business risk on a yearly basis to evaluate whether any changes thereto are necessary.

2.3 Customer Risk Assessment (CRA)

Each customer is assessed individually to determine their risk level based on the following criteria:

- Nature of the customer's business or occupation;
- Source of funds and wealth;
- Geographic location and country risk;
- Products, services, and channels used;
- Transaction behavior and expected account activity;
- Involvement of Politically Exposed Persons (PEPs) or high-risk industries;

Based on the CRA, customers are classified as low, medium, or high risk. The level of due diligence, monitoring, and review is tailored accordingly:

- Low-risk customers are subject to standard due diligence (performed automatically);
- Medium-risk customers require EDD (performed manually);
- High-risk customers are automatically offboarded and are subject to EDD (performed manually) to eliminate errors.

The CRA must be conducted:

- Before entering into any business relationship (e.g., account creation or allowing real-money deposits or gameplay);
- Before processing any occasional transaction equal to or exceeding the monetary threshold;
- Immediately after receiving any new information that may affect the customer's risk profile;
- Whenever a customer's activity or behavior deviates significantly from their established profile;
- Periodically, in accordance with the Company's ongoing monitoring procedures.

2.4 Risk Factor Categories

The company evaluates risks based on the following four primary categories:

- Customer Risk – including type, profile, behavior, source of funds, and whether the customer is a politically exposed person (PEP).
- Geographical Risk – considering exposure to high-risk jurisdictions, sanctioned countries, or areas with weak AML/CFT regimes.
- Product/Service Risk – assessing vulnerabilities linked to the nature of the gaming products and services offered.
- Delivery Channel Risk – including non-face-to-face relationships, use of intermediaries, and digital payment methods.

More detailed factors are outlined in the company's Customer Acceptance Policy.

2.5 Risk Assessment Documentation and Review

The Company shall maintain comprehensive documentation of all Business Risk Assessments (BRA) and Customer Risk Assessments (CRA) conducted as part of its anti-money laundering (AML), counter-terrorist financing (CTF), and counter-proliferation financing (CPF) obligations.

All risk assessments must be fully documented, including:

- Methodology: A clear description of the approach used to evaluate risk across business lines, products, services, geographies, delivery channels, and customer types.
- Risk Factor Rationale: Justification for assigning low, medium, or high-risk ratings to specific risk factors.
- Assessment Outcomes: Final results and conclusions of the assessment, including assigned risk ratings and implications for controls and policies.
- Information Sources: All data, reports, and inputs used to inform the assessment, including internal data, regulatory guidance, industry risk reports, and the National Risk Assessment of Curaçao.
- Risk Appetite Statement: A statement of the level of ML/TF/PF risk the Company is willing to accept, based on the assessment.

These records must be maintained in a retrievable format and made available to the Curacao Gaming Authority (CGA) or other competent authorities upon request.

The Company shall review and update its BRA and CRA documentation at least annually. In addition, event-driven updates must be performed whenever there are significant changes in:

AML Policy (CGA)

Investan N.V.

- The Company's business operations (e.g., new games, markets, payment methods);
- The regulatory environment;
- Risk exposure (e.g., shifts in customer profiles, transaction patterns, or typologies).

The Company shall ensure that its risk assessments remain aligned with the current risk environment and that its AML/CTF/CPF controls are proportionate to the risks identified.

All risk assessment documents must be approved by the Board of Directors or senior management. The Board is responsible for ensuring that the Company's risk management framework is adequate to prevent and mitigate risks of money laundering, terrorism financing, and proliferation financing. Documents must be reviewed at least annually, or more frequently in the event of significant business changes, regulatory updates, or the identification of control weaknesses. All documentation must be maintained in accordance with the company's record-keeping obligations and made available to the Curaçao Gaming Authority upon request.

2.6 National Risk Assessment Integration

The Company is required to incorporate the findings and recommendations of the National Risk Assessment (NRA) of the jurisdiction in which it operates – Curaçao – into its Business Risk Assessment (BRA) process. This integration ensures that the Company's understanding of money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks is aligned with the most up-to-date national-level intelligence and regulatory expectations.

Key Requirements:

- **NRA Consideration:**

The Company shall review the outcomes and recommendations of the Curaçao National Risk Assessment and explicitly consider their relevance when identifying, evaluating, and rating ML/TF/PF risks across its products, services, customer base, delivery channels, and jurisdictions.

- **Incorporation into BRA:**

The findings of the NRA must be reflected in the documented BRA, with clear references to which elements of the Company's risk profile and mitigation strategies were influenced or revised based on the NRA.

As risks are dynamic, the Company must continuously monitor the effectiveness of its internal risk-based approach, including any policy, procedural, or control

AML Policy (CGA)

Investan N.V.

measures that were informed by the NRA. Amendments must be made promptly if new NRA outcomes or emerging threats are identified.

The BRA must be reviewed at least annually, or sooner if significant changes occur in the national threat environment, such as:

- Regulatory updates issued by Curaçao authorities;
- Publication of a new or updated National Risk Assessment;
- Identification of new risk typologies or sectors of concern.

Integration of NRA results into the BRA must be documented, approved by the Board of Directors, and made available to the CGA upon request.

By embedding NRA intelligence into the BRA, the Company ensures that its AML/CTF/CPF risk management framework is both locally responsive and regulatorily compliant, in accordance with Curaçao law and supervisory expectations.

2.7 New Product/Technology Risk Assessment

Prior to the launch of any new product, service, business model, delivery mechanism, or technology, the company must conduct a documented assessment of associated ML/TF risks. This includes:

- Identifying potential threats and vulnerabilities;
- Evaluating how new features may impact existing risk exposure;
- Defining appropriate controls and mitigation strategies.

The results of the assessment, including the methodology, rationale, identified risks, and recommended mitigation controls, must be fully documented. Where higher risks are identified, the Company must develop and implement proportionate mitigating measures, which may include:

- Adjustments to Customer Due Diligence (CDD) procedures;
- Enhanced monitoring protocols;
- Restriction of access to certain customer segments or jurisdictions;
- Additional staff training or technology controls.
- All such risk assessments and mitigation strategies must be:
- Reviewed and approved by the Compliance Officer;
- Escalated to senior management for approval if risk level exceeds the Company's risk appetite;
- Retained and made available to the CGA upon request.

By implementing this forward-looking risk assessment process, the Company ensures

AML Policy (CGA)

Investan N.V.

that technological innovation and business evolution do not compromise its AML/CFT obligations, and that all products and services are introduced in a manner consistent with the Curaçao regulatory framework.

3. GOVERNANCE AND ORGANIZATION

3.1 AML Program Components

The company's AML/CFT program is built upon four foundational pillars, each essential for ensuring the effectiveness, integrity, and compliance of our operations.

Internal Policies, Procedures, and Controls

We have established a comprehensive set of internal AML/CFT policies and procedures designed to detect, prevent, and report suspicious activity. These include risk-based customer due diligence, transaction monitoring, record-keeping, escalation protocols, and safeguards for high-risk areas such as virtual assets and politically exposed persons. The controls are regularly reviewed and updated to remain aligned with evolving regulatory expectations and industry best practices.

- Appointment of a Compliance Officer

A qualified Compliance Officer is designated with the authority and responsibility to oversee the implementation and day-to-day management of the AML program. The Compliance Officer ensures that all regulatory requirements are met, monitors internal adherence to policy, investigates unusual or suspicious activity, and acts as the main liaison with regulators and law enforcement authorities.

- Employee Training and Screening

All relevant employees receive ongoing AML/CFT training tailored to their role and exposure to risk. Training includes identifying red flags, reporting obligations, and understanding typologies of financial crime. In addition, employee screening procedures are in place to ensure the integrity and suitability of individuals working in sensitive or compliance-related functions.

- Independent Audit Function

The AML program is subject to periodic independent audits to assess the adequacy and effectiveness of controls, procedures, and compliance. These reviews are conducted by qualified internal or external parties not involved in daily operations. Findings are documented, reported to senior management, and followed by appropriate remediation actions.

Together, these components form a robust and adaptive AML framework that protects the company from being used as a conduit for financial crime and ensures compliance with applicable legal and regulatory standards.

3.2 Senior Management and Board Responsibilities

AML Policy (CGA)

Investan N.V.

Senior management and the Board of Directors play a critical role in establishing and maintaining an effective AML/CFT framework.

- Approval of the AML Program and Policies

Senior management is responsible for reviewing and formally approving the company's AML program, including all related internal policies, procedures, and controls. This ensures that the program is appropriately designed to address the specific risks associated with the company's gambling operations, customer base, and delivery channels, including the use of digital assets.

- Board Oversight of Risk Assessments and Policy Direction

The board of directors is accountable for overseeing the company's overall approach to AML/CFT risk. This includes the formal approval of the company's risk assessment, risk appetite, and high-level policy direction. The board ensures that sufficient resources are allocated to AML compliance and that the control environment remains effective and responsive to changes in the business or regulatory landscape.

- Communication of ML/TF Risks and Emerging Issues

Senior management must ensure that the board is regularly informed of significant money laundering or terrorist financing risks, internal control deficiencies, regulatory developments, and reputational threats. This includes reporting on suspicious activity trends, audit findings, and key compliance indicators. Timely and transparent communication allows the board to make informed decisions and reinforces the tone from the top.

By actively engaging in the governance of the AML program, senior leadership helps embed a culture of compliance, protect the integrity of the business, and maintain the confidence of regulators, stakeholders, and customers.

3.3 Compliance Officer Appointment and Role

The company formally designated a Compliance Officer at a senior management level to oversee the implementation, maintenance, and effectiveness of the AML/CFT framework. This individual must be functionally independent from the company's gaming operations, free from conflicts of interest, and empowered to carry out their duties without interference.

The Compliance Officer is responsible for:

- Ensuring day-to-day compliance with applicable AML/CFT laws, regulations,

AML Policy (CGA)

Investan N.V.

- and internal policies;
- Coordinating the identification, assessment, and mitigation of money laundering and terrorist financing risks;
- Monitoring the effectiveness of internal controls and procedures;
- Overseeing suspicious transaction detection and reporting processes;
- Acting as the primary liaison with regulators and law enforcement authorities;
- Providing AML-related reporting to senior management and the board;
- Supporting staff training, awareness, and policy enforcement.

The Compliance Officer has unrestricted, timely access to all relevant systems, records, and information necessary to perform his role effectively. He has sufficient authority, resources, and autonomy to ensure the AML/CFT program is implemented consistently and in line with Curaçao regulatory requirements and international standards.

3.4 Compliance Officer Responsibilities

The Company shall formally appoint a Compliance Officer at a senior management level, who is independent from gaming operations and empowered with the necessary authority, access, and resources to effectively oversee the Company's AML/CTF compliance program.

The Compliance Officer must have timely and unrestricted access to all relevant information, including customer identification data, CDD records, transaction logs, and other supporting documents essential for monitoring compliance and conducting investigations.

Core Responsibilities of the Compliance Officer:

- Design, implement, and continuously improve the AML/CFT compliance program.
- Ensure the AML program is risk-based, legally compliant, and aligned with the Company's operational realities.
- Verify adherence to all applicable laws, regulations, guidelines, and directives issued by Curaçao authorities.
- Monitor regulatory changes and initiate program updates when required.
- Periodically review internal policies and procedures for adequacy and effectiveness.
- Recommend modifications in response to risk changes or compliance gaps.
- Organize and oversee AML training programs for all relevant staff.
- Ensure staff remain informed about current ML/TF/CPF typologies and legal obligations.

AML Policy (CGA)

Investan N.V.

- Analyze customer transactions to identify anomalies or red flags suggesting potential ML/TF activity.
- Maintain systems and procedures for proactive monitoring and detection.
- Review all internally reported unusual transactions (UTRs).
- Determine whether reports meet the threshold for external reporting.
- Conduct closer investigations of suspicious activity.
- Escalate cases where reporting or account intervention (e.g., suspension or freezing) may be required.
- Prepare and submit reports of unusual transactions to the Financial Intelligence Unit (FIU) through the goAML portal.
- Maintain an audit trail of all communications with the FIU.
- Ensure all records related to CDD, transactions, UTRs, training, and investigations are properly maintained for at least five years.
- Verify that documentation is complete, accurate, and readily available for inspection by authorities.
- Recommend and implement necessary changes to the AML program based on emerging risks, audit results, or regulatory feedback.
- Stay informed on developments in legislation, enforcement trends, and international best practices.

The Compliance Officer's duties and responsibilities shall be formally defined in a written job description. This job description shall be signed and dated by the appointed officer to confirm acceptance of the assigned duties.

3.5 Internal Controls Framework

The company established and maintained a robust internal controls framework to ensure effective implementation of its AML/CFT obligations and to support the Compliance Officer in identifying, preventing, and addressing any procedural deviations or control weaknesses.

These internal controls must:

- Be clearly documented, risk-based, and integrated across all relevant departments and operational processes;
- Enable the Compliance Officer to detect and respond to failures, gaps, or inconsistencies in the application of AML/CFT procedures;
- Include monitoring mechanisms for ongoing evaluation of control effectiveness and compliance with regulatory requirements;
- Provide for escalation procedures in cases of significant breaches or suspected non-compliance.

AML Policy (CGA)

Investan N.V.

The Compliance Officer is responsible for overseeing the implementation and continuous improvement of internal controls, ensuring they remain aligned with the evolving risk environment and industry standards.

Where higher risks are identified—such as customers from high-risk jurisdictions, politically exposed persons (PEPs), or unusual transaction patterns—enhanced internal measures must be applied. These may include strengthened due diligence, additional approval layers, more frequent transaction reviews, and tailored monitoring protocols.

The internal controls framework is a cornerstone of the company's AML/CFT program, ensuring that regulatory compliance is proactive, auditable, and continuously improved over time.

3.6 Process for Regulatory Updates

The Company has developed its policies and procedures in accordance with applicable legislation and the guidance of the FATF, CGA, and FIU. However, both regulatory requirements and external fraud trends are subject to change. To ensure the ongoing relevance of the Company's internal AML documentation, the following measures have been implemented:

- Key personnel have subscribed to mailing lists from the FIU, CGA, and FATF and have joined relevant forums to stay informed.
- The Company periodically consults Remote gaming industry specialists for legal advice on AML best practices.

In the event of an update, the Company will take the following actions as necessary:

- Update internal policy documentation and training materials;
- Notify relevant staff via email of any updates, meet with team managers, and ensure they inform their teams appropriately;
- Update email communication templates and chat canned response;
- Update website policies, maintaining version numbers and "last updated" dates;
- Update the Terms and Conditions, maintaining a version number and 'last updated' date.

Any updates to the Terms and Conditions will trigger a pop-up notification for players upon their next login, requiring them to accept and agree to the new version before proceeding.

The Company may also engage a third-party service provider specialising in AML compliance to conduct independent external reviews of its AML policies and

AML Policy (CGA)

Investan N.V.

procedures. The results of these reviews will be reported to senior management and used to enhance the Company's AML/CTF measures and documentation as needed. The frequency of these external reviews will be determined by senior management. They may occur annually or more frequently, depending on the need for updated assessments of the AML program's effectiveness.

4. CUSTOMER DUE DILIGENCE FRAMEWORK

4.1 CDD Principles and Prohibitions

In accordance with AML/CFT regulations applicable to the Company operating under the laws of Curacao, CDD measures are implemented in cases when a player engages in transactions that meet or exceed the designated threshold amount. Anonymous or fictitious accounts are prohibited

The Company differentiates between Customer Due Diligence (CDD) and Enhanced Customer Due Diligence (EDD).

Customers are required to cooperate in fulfilling the due diligence obligations. If the Company is unable to complete the necessary due diligence, the business relationship will not be initiated or continued, and no transactions will be processed. Furthermore, the Company will assess whether it is necessary to file a Suspicious Activity Report (SAR).

4.2 CDD Triggering Events and Thresholds

Pursuant to the guidelines any transaction (single or linked) equal to or exceeding NAf 4,000 or its equivalent EUR 2,000 (as operational currency of the company accounting and reporting) shall trigger mandatory CDD procedures namely identity verification and obtaining of document information on the source of funds.

CDD must be conducted in the following circumstances:

- When a financial or occasional transaction (or a series of linked transactions) equals or exceeds NAf. 4,000 or its equivalent EUR 2,000;
- When there is a suspicion of money laundering or terrorist financing, regardless of the amount;
- When there are doubts about the veracity or adequacy of previously obtained customer identification data;
- When establishing a new player account or entering into a continuing business relationship.

For linked transactions, the cumulative value within a 24-hour period must be considered when assessing if the threshold is met.

4.3 CDD Measures Overview

To finalize registration, the customer must successfully pass the Customer Due Diligence (CDD) process. If the CDD is not passed, the registration will be denied.

The process cannot take more than 72 hours from the time the customer sends the information.

The company's CDD process includes the following key measures:

- Identifying and verifying the identity of the customer using reliable, independent sources;
- Identifying and verifying the identity of the beneficial owner where applicable;
- Understanding the nature and purpose of the business relationship to establish a customer risk profile;
- Conducting ongoing due diligence, including transaction monitoring and periodic review of customer data.

4.4 Customer Identification Requirements

At minimum, the following information must be collected during account registration:

- Full legal name;
- Residential address;
- Date of birth (DOB);
- Place of birth (POB);
- Nationality;
- Government-issued identification number.

For low-risk customers, simplified due diligence may allow for the collection of just name, address, and DOB. In high-risk situations, additional data must be collected to appropriately assess the customer's profile.

4.5 Customer Verification Requirements

As part of its CDD obligations, the Company must verify the identity of each customer by referencing reliable and independent sources. The purpose of this verification is to

AML Policy (CGA)

Investan N.V.

ensure that the customer exists and is who they claim to be, thereby mitigating the risks associated with money laundering, terrorist financing, and identity fraud.

Identity verification must be performed using unexpired government-issued documents that contain:

- The customer's full name,
- A photograph, and
- A signature.

Acceptable documents include, but are not limited to:

- A national identity card,
- A passport,
- A driver's license (with photo and signature),
- Any other equivalent official documentation issued by a government authority.

If the government-issued identification document does not include a residential address, the customer must provide a secondary document to confirm their address. These documents must be dated within the last six (6) months and may include:

- A utility bill,
- A bank statement,
- A letter from a public authority,
- A tax statement, or
- A rental or lease agreement.

The Company may perform additional verification by:

- Contacting the customer by email, phone, or post to confirm the information provided,
- Sending a verification code to the registered email address or phone number,
- Requiring the customer to upload a selfie holding their identification document, or
- Requesting a first deposit made from a financial account in the customer's name, preferably from a reputable jurisdiction.

Where the Company does not have sufficient comfort that it fully knows the identity of a customer — particularly when risk factors or inconsistencies are present — enhanced verification measures must be applied. This may include:

- Collecting additional identity documentation,
- Conducting a video verification session, or
- Obtaining proof of source of funds or source of wealth.

4.6 Beneficial Owner Requirements

The company takes reasonable steps to identify and verify beneficial owners of any account, and to ensure that customers are playing on their own behalf. Continuous monitoring procedures must be in place to detect possible third-party use of accounts. The company makes sure that customers are registering an account to play and transact on their behalf.

Depending on the risk level, the Company may rely on a combination of customer declaration, CDD/EDD information and ongoing monitoring procedures to detect behavior that could indicate third-party usage.

If third-party activity is suspected, enhanced due diligence must be initiated and the account may be subject to suspension or termination, subject to further investigation.

These measures are integral to the effectiveness of the Company's AML/CFT framework and its risk-based approach to customer due diligence.

4.7 Business Relationship Purpose and Customer Profiling

The company must establish the purpose and intended nature of the business relationship and build a risk-based customer profile. This includes gathering information on:

- Source of wealth and, where applicable, source of funds;
- Expected volume and nature of gaming activity;
- For high-risk customers, such information must be verified using independent documentation;
- For standard-risk customers, a declaration may suffice unless risk triggers further review.

4.8 CDD Timing and Account Management

The company must apply CDD measures in a timely and risk-sensitive manner, aligned with the Curaçao AML regulatory requirements. The timing of CDD implementation is directly tied to the establishment of the business relationship and the financial activity of the customer.

At the time of account registration, before any deposit or gameplay occurs, the following minimum CDD information must be collected:

AML Policy (CGA)

Investan N.V.

- Full name and surname;
- Permanent residential address;
- Date of birth (DOB);

In addition, the following mandatory screenings must be conducted:

- Sanctions screening (UN, EU, Curaçao lists);
- PEP (Politically Exposed Person) status screening.

Accounts may not be activated for real-money deposits or withdrawals until this minimum CDD is complete and the customer is cleared through both screenings.

The company must conduct full CDD measures – including identity verification, beneficial ownership checks (if applicable), customer risk assessment, and source of funds inquiries – once the player's financial activity equals or exceeds NAf. 4,000.

The NAf. 4,000 threshold is calculated on a daily basis, considering all deposits, withdrawals, and peer-to-peer transfers from the beginning of the business relationship. Once this threshold is reached or exceeded, the full CDD process must be completed without delay.

Different restrictions apply depending on how the NAf. 4,000 threshold is reached:

- If the threshold is reached due to a deposit:

The customer is not allowed to make further deposits or withdrawals until full CDD is completed.

However, the customer may continue to play using the funds already in the account.

- If the threshold is reached due to a withdrawal request:

The customer's account must be completely frozen, meaning no withdrawals, no deposits, and no gameplay are permitted.

The freeze remains in effect until all required CDD documentation and verification are completed and approved.

These procedures ensure that financial activity above the risk-sensitive threshold does not proceed without full verification of the customer's identity and legitimacy.

4.9 Enhanced Due Diligence (EDD)

EDD must be conducted in the following scenarios, among others:

- When a player is resident in or transacts from a high-risk jurisdiction or geographic area (as defined in relevant FATF or national risk lists).
- When a customer uses or engages in products or transactions that favor

AML Policy (CGA)

Investan N.V.

anonymity (e.g. use of privacy-enhancing cryptocurrencies, anonymous prepaid cards).

- When the customer is using or being onboarded for new products, business models, or delivery mechanisms that the casino has not previously assessed.
- When an occasional transaction presents a high risk of ML/TF due to its size, pattern, or associated party.
- Where the customer or transaction otherwise triggers high-risk indicators in the casino's Business Risk Assessment or Customer Risk Assessment.

The scope and nature of the EDD measures applied must be proportionate to the specific risks identified. These may include:

- Obtaining additional information on the customer (e.g. employment, background, ownership structure).
- Gathering more detail about the intended nature and purpose of the business relationship.
- Verifying the source of funds (SoF) and/or source of wealth (SoW) of the player.
- Requesting an explanation for the reasons behind certain transactions or transaction patterns.
- Requiring senior management approval prior to establishing or continuing the business relationship.
- Implementing enhanced ongoing monitoring of the customer's transactions and gameplay behavior.

In higher-risk customer relationships, even in the absence of new behavioral triggers or changes in activity, the casino must periodically request updated source of funds documentation to ensure that the business relationship remains legitimate and consistent with the declared purpose.

These requirements aim to ensure that higher-risk scenarios are met with greater scrutiny and ongoing oversight in order to prevent abuse of the gaming environment for illicit purposes.

4.10 Simplified Due Diligence (SDD)

Where the risk of money laundering or terrorist financing is assessed to be low, the Company may apply Simplified Due Diligence (SDD) measures. These measures must be proportionate to the nature and level of the lower risk and shall not compromise the Company's ability to understand the customer and the purpose of the relationship.

Examples of simplified measures include:

- Limited information collection: If the customer is classified as low-risk based

AML Policy (CGA)

Investan N.V.

on a documented risk assessment, the Company may collect only essential identification information. In such cases, identification may be limited to the customer's full name, date of birth, and residential address.

- Delayed verification: The verification of the customer's and, where applicable, the beneficial owner's identity may be completed after the establishment of the business relationship, provided that this does not conflict with regulatory obligations.
- Risk-adapted verification sources: The Company may rely on alternative, reputable sources of information for identity verification in low-risk situations, even if such sources lack photographic evidence (e.g., birth certificates, utility bills, or bank statements).
- Limited extent of verification: In low-risk scenarios, only the basic identification data must be verified. Additional personal details may be verified at the Company's discretion, as long as there is sufficient assurance that the identity of the customer is known.
- Reduced frequency of updates: The Company may apply a reduced frequency for updating customer identification records and documentation.
- Lower intensity of ongoing monitoring: Ongoing monitoring activities may be less frequent and less detailed, based on pre-defined monetary thresholds and risk triggers.

Simplified Due Diligence measures must not be applied where there is a suspicion of money laundering or terrorist financing, or where high-risk indicators are present (e.g., PEP status, high-risk jurisdiction, adverse media, unusual transactions). In such cases, full standard or enhanced due diligence procedures shall apply.

4.11 Politically Exposed Persons (PEPs)

A Politically Exposed Person (PEP) is an individual who holds or has held a prominent public position at the international, national, or subnational level. This includes, but is not limited to:

- Heads of state or government;
- Ministers, deputy and assistant ministers;
- Members of parliament and other legislative bodies;
- Senior government, judicial, military, and law enforcement officials;
- High-ranking members of central banks, courts of audit, and constitutional courts;
- Ambassadors and defence attachés;
- Executives or board members of state-owned enterprises;
- Senior officials of international or intergovernmental organizations (e.g., UN,

AML Policy (CGA)

Investan N.V.

- EU);
- Family members of PEPs are also considered high-risk and subject to Enhanced Due Diligence. This includes:
 - Spouse or registered partner;
 - Children and their spouses or partners;
 - Parents of the PEP.

The Company considers both domestic and foreign PEPs, and applies the PEP designation for a minimum of 12 months following the termination of a public role (the “post-PEP” period).

All new customers are screened for PEP status during the onboarding process using specialized KYC/AML software that accesses updated international PEP and Sanctions databases.

The full customer database is rescreened at least every six months to identify changes in PEP or sanctions status.

If a PEP match is detected, the case is escalated to the Compliance Officer for review.

The Compliance Officer verifies whether the match is a true positive or a false positive. If needed, the customer may be asked to provide additional documentation (e.g., source of wealth, official confirmation of occupation).

If confirmed as a PEP or relative, the account will either be rejected or closed, based on risk assessment and senior management decision.

All players must be screened against the sanctions lists issued by the United Nations (UN) and the European Union (EU), Curacao local list prior to onboarding or conducting any transaction:

- UN Consolidated Sanctions List:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

- EU Sanctions Map:

<http://www.sanctionsmap.eu/#/main>

The Company utilizes automated KYC tools and/or manual searches to cross-check player data against these lists. Any confirmed match results in immediate account rejection or closure, and, if appropriate, a report to the Financial Intelligence Unit (FIU).

To assess whether a player is a PEP or associated with a PEP, the Company conducts screening during onboarding and periodically thereafter.

The Company applies EDD to any player identified as a current or former PEP, or a close associate or family member of a PEP.

Customers or entities identified on a sanctions list are immediately flagged and

AML Policy (CGA)

Investan N.V.

reported to the Compliance Officer. Verified positive matches result in immediate account rejection or closure, and may require a Suspicious Activity Report (SAR) to be filed with the Financial Intelligence Unit (FIU).

Adverse media includes any credible negative information indicating that a person or entity may be involved in:

- Criminal activity (e.g., fraud, money laundering, terrorism);
- Regulatory violations or sanctions evasion;
- Corruption or reputational risk.

Sources of adverse media may include news agencies, court records, government publications, regulatory notices, or other publicly available reliable sources.

Customers identified in adverse media screenings are automatically subject to Enhanced Due Diligence (EDD) procedures.

Based on the outcome of the EDD, the Company may decide to reject account registration, restrict activity, or close the account.

4.12 Ongoing Monitoring

The general due diligence duties include ongoing monitoring of the business relationship. This involves:

- Obtaining updated identification when existing documents expire (this can be done on a risk-sensitive basis);
- Investigating any data or information inconsistencies noticed by the Company;
- Conducting periodic reviews and updates based on risk sensitivity;
- Ensuring transactions align with the documents and information the Company holds about the customer, including the customer's assets and the origin of funds;
- Updating relevant documents, data, or information at appropriate intervals.

To ensure customer information remains current, the Company conducts the ongoing CDD procedure at least once every 12 months, or more frequently at its sole discretion, based on a risk-sensitive approach.

4.13 Existing Customer Application

The company must apply CDD measures not only to new customers but also to existing customer relationships, based on risk and materiality.

AML Policy (CGA)

Investan N.V.

Where appropriate, the Company shall perform CDD on existing customers in a risk-sensitive and proportionate manner, ensuring that due diligence measures are applied at relevant trigger points, such as:

- A significant change in the customer's profile, behavior, or transaction pattern;
- A new risk factor identified (e.g., emerging PEP status, sanctions listing, adverse media);
- A scheduled periodic review based on the customer's risk rating;
- Regulatory changes or audit findings requiring customer file updates.

In cases where no prior CDD procedures were applied (e.g., due to legacy onboarding), the Company is required to retroactively apply CDD measures in line with current regulatory standards and internal policies. This process must also follow a risk-based approach, prioritizing higher-risk relationships for immediate review.

4.14 Business Relationship Termination

The Company is obligated to refuse to establish a business relationship or terminate an existing relationship with any customer when the CDD obligations cannot be fulfilled, including failure to obtain sufficient identification information, documentation, or verification of the customer or the beneficial owner.

It is important to note that a customer's reluctance or delay alone in providing CDD documentation does not automatically constitute suspicion of ML/TF/FP. However, this factor may contribute to an overall suspicion when considered alongside other behavioral or transactional indicators.

Where the risk of ML/TF/FP cannot be reasonably mitigated, or where suspicion arises during this reassessment, the Compliance Officer must be notified, and appropriate actions—such as filing a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU Curaçao)—must be considered.

4.15 Third Party Reliance

In limited circumstances, the Company may rely on third parties to perform certain elements of the Customer Due Diligence (CDD) process, specifically elements defined below:

- Identification of the customer;
- Verification of the customer's identity;
- Identification and verification of the beneficial owner (where applicable);

AML Policy (CGA)

Investan N.V.

- Sanctions, PEP, adverse media screening.

However, such reliance is only permissible where all of the following criteria are met, and the ultimate responsibility for compliance with the CDD requirements remains with the Company:

- Immediate Availability of CDD Information:

The Company must obtain all relevant CDD information (elements a–c) without delay from the third party upon onboarding the customer.

- Access to Supporting Documentation:

The Company must have a written agreement or understanding in place with the third party, ensuring that copies of identification data and other relevant documentation will be made available immediately upon request, whether for internal audit, regulatory review, or investigative purposes.

- Regulatory Status of the Third Party:

The third party must be a legal entity that is subject to regulation, supervision, or monitoring for AML/CFT compliance in its jurisdiction. The Company must be reasonably satisfied that the third party has robust measures in place for fulfilling its obligations regarding CDD and recordkeeping.

- Country Risk Assessment:

The Company must assess the jurisdiction in which the third party is based, taking into account publicly available information (e.g., FATF mutual evaluation reports, EU listings, country risk indices) to ensure the jurisdiction has adequate AML/CFT standards. Third parties located in high-risk jurisdictions may not be relied upon unless additional safeguards are in place.

Where the Company chooses to rely on a third party under these conditions, such reliance must be clearly documented, and the decision should be periodically reviewed by the Compliance Officer to ensure continued compliance and integrity of the CDD process.

4.16 Tipping-Off Considerations

It is a criminal offense to inform anyone that a SAR has been submitted or is being considered if doing so could prejudice the investigation. While internal discussions about the customer are permitted, neither the customer nor their associates should be made aware that the customer may be under investigation.

This means that no employee of the Company:

AML Policy (CGA)

Investan N.V.

- Can inform a customer that a transaction is being delayed because a report is pending approval (consent) from the FIU;
- Can disclose to the customer that law enforcement is conducting an investigation.

4.17 Sanctions Framework

The Company complies with all targeted financial sanctions obligations, including those imposed by the United Nations, the European Union, and any applicable sanctions lists issued by the authorities of Curaçao.

In accordance with legal requirements, the Company is obligated to:

- Immediately freeze, without delay and without prior notice, any funds or assets belonging to individuals or entities listed on sanctions lists;
- Prevent any funds, assets, or economic resources from being made directly or indirectly available to or for the benefit of any designated persons or organizations.

All relevant departments, including payments, risk, compliance, and operations, are required to be familiar with these obligations and follow internal procedures for identifying and responding to potential sanctions matches.

5. TRANSACTION MONITORING AND REPORTING

5.1 Unusual Transaction Recognition Framework

The Company maintains comprehensive procedures to ensure the effective recognition, documentation, and reporting of both completed and intended unusual transactions, in accordance with Curaçao's National Ordinance on the Reporting of Unusual Transactions (NORUT).

The key to detecting unusual transactions lies in having a robust understanding of the customer. This is achieved through the development of individual player profiles during the CDD process and through continuous behavioral monitoring. Knowing the player's typical patterns and expected activity allows staff to identify deviations that may indicate ML/TF or other suspicious behavior.

All internal reports of unusual transactions are to be submitted without delay to the Compliance Officer using approved reporting formats and must be accompanied by relevant supporting documentation.

5.2 Unusual Transaction Categories

In line with regulatory requirements, the following transactions – whether completed or attempted – must be treated as unusual:

- a. Transactions linked to ML/TF that are reported to law enforcement authorities;
- b. Transactions involving persons or entities listed under any sanctions ordinance;
- c. Transactions equal to or exceeding NAf. 5,000 (or the equivalent in another currency), including:
 - Cashless deposits
 - Chip purchases
 - Withdrawals
 - Other combinations or patterns of transactions conducted within a single gaming day;
- d. Transactions presumed to be linked to ML/TF based on indicators such as structure, amount, frequency, or customer profile.

The NAf. 5,000 threshold applies not only to single transactions but also to linked transactions conducted over the same gaming day. Monitoring systems must calculate

cumulative transaction values daily to detect threshold breaches.

5.3 Staff Training and Internal Reporting

The Company's management is responsible for ensuring that all relevant employees are trained to recognize, assess, document, and internally report unusual transactions. This includes:

- Practical instruction on transaction indicators and typologies;
- How to use internal reporting tools and documentation templates;
- Guidance on preserving confidentiality and avoiding tipping-off.

All internal unusual transaction reports (UTRs) must be submitted to the Compliance Officer immediately upon identification, along with all relevant supporting records such as:

- Player identification documentation;
- Transaction logs or receipts;
- Communications or behavioral notes.

The Compliance Officer maintains a centralized filing and tracking system for all UTRs and supporting documentation.

5.4 Complex and Large Transaction Monitoring

In accordance with FATF Recommendation 11, the Company pays special attention to:

- Complex or unusually large transactions;
- Unusual patterns of activity;
- Transactions that appear to lack a clear economic or lawful purpose.

Transactions meeting these criteria are subject to enhanced scrutiny and must be escalated to the Compliance Officer. If suspicion of ML/TF arises, an internal UTR is filed immediately and assessed for potential external reporting.

5.5 External Reporting Procedures

The Company is registered with the FIU Curaçao and maintains access to the goAML

online reporting portal.

The Compliance Officer is responsible for:

- Preparing and submitting reports of unusual transactions (including attempted transactions) without delay;
- Ensuring that all required data fields are completed and that reports are submitted in English, as mandated;
- Including all supporting documentation (e.g., IDs, screenshots, withdrawal receipts) with the report submission.

All reports must comply with the FIU's technical and legal requirements, and submission must occur without undue delay upon confirmation of the unusual nature of the transaction.

5.6 Internal Decision Documentation

If the Compliance Officer or management determines that an internally reported transaction does not warrant external reporting to the FIU, this decision must be:

- Formally documented with the rationale for non-reporting;
- Signed off by the Compliance Officer and/or designated senior management;
- Retained in the transaction monitoring records for audit and review purposes.

This ensures traceability, accountability, and compliance with the principle of proper internal governance.

5.7 Disclosure Prohibitions and Tipping-Off

Under Curaçao AML/CFT law and the provisions of the Sanctions Ordinance, all employees, managers, and agents of the Company are strictly prohibited from disclosing:

- That a report has been or will be submitted to the FIU;
- The content of the report or the identity of the person involved;
- Any inquiry made by the FIU.

This prohibition applies to the customer and to any third party. To avoid tipping off, staff must exercise caution when taking operational steps following a report to the FIU. Where possible, drastic action (e.g., account closure) should be deferred or replaced with enhanced monitoring unless a clear legal obligation or security concern

AML Policy (CGA)

Investan N.V.

justifies immediate action.

If further suspicious activity is observed, additional reports should be submitted to the FIU to supplement the original disclosure.

6. TRAINING AND AWARENESS

6.1 Training Program Framework

The Company is committed to maintaining a robust and effective AML/CTF training program. This program is designed to ensure that all employees, especially those handling transactions or customer interactions, are fully aware of their responsibilities in identifying, reporting, and mitigating ML/TF risks.

Training initiatives shall include:

- Education on the rules of conduct and the ethical standards required of all staff;
- Awareness of ML/TF typologies, indicators, and trends specific to the gambling sector;
- Continuous professional development to ensure that staff remain updated on evolving threats and compliance obligations.

Training must be conducted across all operational departments and adapted to specific job roles.

6.2 Employee Screening

As part of its internal control environment, the Company maintains pre-employment screening, which includes:

- Criminal background checks for all new hires;
- Evaluation of integrity and past conduct relevant to financial crime risks;
- Periodic re-screening where necessary for employees in sensitive or high-risk positions.

This ensures that individuals with a known history of financial crime are not placed in roles where they could compromise the integrity of the AML program.

6.3 Role-Specific Training Requirements

Training content is tailored to the specific responsibilities of each employee category.

Each training module must be aligned with the employee's job duties and the specific risks they may encounter.

6.4 New Employee Training

All new employees who handle customers or transactions must receive mandatory AML/CTF onboarding training, covering:

- The nature, purpose, and stages of money laundering and terrorist financing;
- CDD procedures and customer profiling;
- Objective and subjective indicators for detecting unusual transactions;
- Procedures for reporting suspicious activity;
- Common ML/TF methods used in the gambling sector.

This training must be delivered before the employee begins handling transactions or customer accounts.

6.5 Front-Line Staff Training

Support personnel shall undergo practical training that includes:

- The importance of AML compliance;
- How casinos may be exploited by money launderers;
- Recognition of red flags and high-risk behaviors;
- Customer identity verification obligations;
- Steps to take when unusual activity is observed.

Front-line staff must be trained to escalate issues promptly and discreetly to compliance personnel.

6.6 Specialized Training

Audit staff responsible for monitoring, testing, and assessing AML controls must be trained on:

- Updates in AML/CTF regulations and enforcement actions;
- New ML/TF typologies and threats;

- Risk mitigation techniques and internal testing procedures.

AML compliance officers shall receive advanced, specialized training to stay abreast of:

- Emerging threats and typologies;
- Legislative and regulatory changes affecting the gaming sector;
- Enhanced risk assessment and reporting requirements.

6.7 Management Training

Supervisors and managers are required to undergo advanced AML/CTF training, which includes:

- A comprehensive overview of AML/CTF laws, regulations, and responsibilities;
- Oversight and enforcement of staff compliance;
- Internal investigation procedures;
- Managing escalated ML/TF risks and internal reporting protocols.

Senior management and board members must be regularly briefed on:

- Major AML/CTF issues, including reputational risks;
- Strategic impact of non-compliance;
- Internal audit results and FIU reporting activity.

This ensures top-level accountability and informed governance.

6.8 Refresher Training

To maintain awareness of the dynamic nature of financial crime, refresher training shall be provided at regular intervals, and at minimum annually. This includes:

- Updates on ML/TF trends, schemes, and typologies;
- Review of reporting procedures and CDD standards;
- Re-training on amended policies and regulatory changes;
- Lessons learned from internal cases or external enforcement actions.

Employees must demonstrate continued competence via periodic testing and assessments.

6.9 Training Documentation

To demonstrate compliance with training requirements, the Company maintains a training records management system. For each training activity, the following information must be retained:

- Content of the training session;
- Names and roles of attendees;
- Date and delivery method of training;
- Results of any assessments or evaluations;
- Planned dates for future training (ongoing training plan).

These records are retained for a minimum of five years and are available for inspection by regulators or auditors upon request.

7. AUDIT AND INDEPENDENT REVIEW

7.1 Independent Audit Requirements

The Company shall ensure that its AML/CTF compliance program is subject to formal monitoring and evaluation at least once per year. This audit must be conducted by either:

- A qualified internal audit function, or
- An independent third-party reviewer, who has no direct or indirect involvement in the AML compliance function or day-to-day operations of the program.

Auditors must possess sufficient professional qualifications, expertise, and independence to perform an objective and comprehensive evaluation of the AML framework. This ensures that the audit results are reliable and support risk-based oversight by management and regulatory authorities.

7.2 Audit Scope and Testing

The AML audit must be comprehensive in scope and include both compliance review and effectiveness testing of the following program elements:

- Evaluation of the Company's AML/CTF/CFP policy manuals and procedures;
- Review of the effectiveness and governance of the compliance management structure;
- Transaction sampling and testing for proper detection and escalation of unusual or suspicious activity;
- Evaluation of the employee training program and adequacy of its implementation across departments;
- Assessment of compliance with Curaçao's National Ordinance, Decrees, and any applicable EU/UN requirements;
- Sampling and review of internally reported UTRs and decisions made;
- Assessment of the record-keeping and retention system, including audit trails and supporting documentation;
-
- Employee interviews to assess AML/CTF knowledge, application of internal procedures, and escalation practices.

All elements must be tested with the purpose of verifying whether the AML program is functioning effectively in both theory and practice.

7.3 Audit Documentation and Reporting

The results of the audit must be thoroughly documented. This includes:

- The scope of the audit, methodology used, and personnel interviewed;
- A summary of findings, including strengths and deficiencies;
- A list of non-compliance issues, gaps, or control weaknesses identified;
- Recommendations for corrective action and deadlines for implementation.

These results must be reported to:

- The Compliance Officer;
- Senior Management; and
- The Board of Directors or Supervisory Board, where applicable.

Management is responsible for ensuring that all deficiencies are addressed promptly and that corrective actions are monitored to completion.

7.4 Program Testing and Adaptation

In accordance with Curaçao's regulatory expectations, the Company regularly tests the AML program against emerging internal and external risks. Program testing should be systematic and risk-based, taking into account:

- Recent changes in regulatory requirements;
- Modifications to internal systems or business lines (e.g., new payment methods, jurisdictions, or customer types);
- Identified ML/TF typologies or industry trends;
- Compliance feedback received from regulators or audit results.

Where risks or operational developments justify updates to the AML framework, the Company will adapt its internal controls, procedures, and risk assessments accordingly.

Any updates or revisions to the AML program must receive formal approval from senior management, and staff must be trained accordingly to ensure proper implementation.

8. RECORDS AND DOCUMENTATION

8.1 Record Retention Requirements

The Company shall retain all transaction and CDD records in accordance with Curaçao's legal and regulatory framework.

Transaction Records: All necessary information related to domestic and international transactions, including the nature, amount, date, method of payment, and account details involved, shall be retained for a minimum of five (5) years following the execution of the transaction. These records must be sufficient to reconstruct individual transactions to support law enforcement investigations and criminal prosecutions if needed.

CDD Records and Account Files: All records obtained through CDD processes – such as identification documents, account files, source of funds data, business correspondence, and supporting documents – shall be kept for at least five (5) years from the date:

- The business relationship ends; or
- The occasional transaction is completed.

These retention requirements ensure that the Company maintains adequate evidence of its compliance obligations and can support requests by competent authorities during investigations or regulatory reviews.

8.2 Regulatory Access Requirements

All CDD and transaction records must be made readily available to the relevant supervisory authorities, including but not limited to:

- The Financial Intelligence Unit (FIU);
- The Curacao Gaming Authority (CGA);
- Other competent domestic authorities operating under appropriate legal authority.

The Company is obligated to ensure timely access to these records to facilitate examinations, audits, investigations, or law enforcement proceedings.

The Company must implement systematic, organized storage and retrieval systems that allow for quick response to information requests by competent authorities.

8.3 CGA Examination Documentation

In preparation for or during an examination by the Curacao Gaming Authority (CGA), the Company must make the following items readily available upon request:

1. The written and Board-approved AML Compliance Program;
2. A current and historical Business Risk Assessment (BRA), including:
 - Methodologies used;
 - Risk ratings assigned to factors (low, medium, high);
 - Justifications for risk classifications;
 - Data sources and national risk assessment outcomes considered;
3. Records related to the appointment and role of the Compliance Officer;
4. Logs of all UTRs filed internally and/or externally;
5. Records of any investigations triggered by internal UTRs;
6. Documentation regarding any frozen or blocked accounts as a result of sanctions or suspicious activity;
7. Employee training schedules and records (topics, attendance, testing results);
8. Audit reports issued by internal or external auditors on AML program effectiveness;
9. Records of Customer Risk Assessments (CRA), including:
 - CDD results;
 - Customer Acceptance documentation;
 - Transaction history and associated monitoring notes.

All documentation listed above must be stored in a manner that ensures integrity, security, and timely retrieval, and retained in accordance with the regulatory timeframes outlined under Section 9.1.

8.4 Documentation Standards

The Company shall maintain comprehensive and well-organized documentation of all compliance-related activities, risk assessments, and internal procedures to ensure transparency, accountability, and adherence to Curaçao's AML/CFT regulatory framework.

All documentation must be stored securely and retained for the period required by law (at least five years) following the end of the business relationship or the execution of an occasional transaction, in accordance with Curaçao's Record Retention and BRA Requirements.

The documentation must be readily accessible for review by competent authorities, including the CGA and FIU, upon request.

9. POLICY MAINTENANCE AND REVIEW

9.1 Policy Review and Updates

The Company is committed to maintaining its AML/CTF/CFP framework in line with applicable laws, regulations, and industry standards.

To ensure continued effectiveness:

- The AML Policy and related procedures shall be reviewed at least annually
- Additional reviews shall be conducted following significant changes in:
- Applicable legislation or regulatory guidance;
- The Company's business operations, products, or delivery channels;
- Identified risks based on audits, internal reports, or supervisory feedback.

A designated Compliance Officer is responsible for monitoring regulatory developments and initiating updates to ensure the AML program remains current and compliant.

All updates must be documented, dated, and stored appropriately.

9.2 Policy Approval and Communication

The AML Policy and all material amendments thereto shall be:

- Approved by the Board of Directors or Senior Management;
- Formally documented with version control, approval dates, and the names of approving officials.

Once approved, the AML Policy shall be:

- Distributed to all relevant staff members;
- Accompanied by targeted training or briefings, especially when policy changes impact roles and responsibilities;
- Available in an accessible format for reference by employees at any time.

The Compliance Officer is responsible for ensuring policy communication and staff understanding.

9.3 Non-Compliance and Escalation

Any deviation from AML/CFT policies or procedures, whether intentional or unintentional, is treated seriously.

The Company has implemented an escalation process that includes:

- Immediate internal reporting of suspected or actual non-compliance to the Compliance Officer;
- Investigation of the incident and documentation of findings;
- Corrective actions taken and controls implemented to prevent recurrence;
- Escalation to senior management or the Board, where the breach may pose regulatory, financial, or reputational risk;

Disciplinary measures, if warranted, in accordance with the Company's HR and internal compliance frameworks.

Non-compliance incidents are analyzed to improve internal controls and update policies where necessary.

Signed by:

D94CF92AB2FF4F2...